



RHODES UNIVERSITY

Where leaders learn

**Investigating the Use of Nudging to Dissuade Online
Banking Fraud**

by

Takudzwa Mutyavaviri

Investigating the Use of Nudging to Dissuade Online Banking Fraud

By

Takudzwa Mutyavaviri

G17M0239

ORCID <https://orcid.org/0000-0002-9227-1283>

Thesis

submitted in fulfilment of the requirements for the degree

Master of Commerce

in

Information Systems

in the

Faculty of Commerce

of

Rhodes University

Supervisor: **Dr K. van der Schyff**

Supervisor: **Prof. K. Renaud**

January 2023

ABSTRACT

Online banking is a service offered by most modern banks to provide their clients with a convenient means to access their bank accounts remotely. However, such convenience comes at a cost and has the potential to expose clients to online banking fraud. To mitigate such forms of fraud, banks make extensive use of traditional cybersecurity measures such as firewalls, intrusion detection systems, as well as personal identification numbers (PINs) and passwords. However, despite the use of such traditional cybersecurity measures, online banking fraud still occurs. In particular, traditional cybersecurity measures have difficulties detecting the unauthorised use of a customer's online banking credentials.

For this reason, this study's main objective was to investigate the effectiveness of nudges when used to dissuade the unauthorised use of clients' online banking credentials. The study also had two secondary objectives: firstly, to identify where the deployment of nudges would be most effective; and secondly, to identify the rationalisations an individual may use to justify committing online banking fraud. Although previous research has sought to understand the use of nudges in various online contexts, none have done so within the context of online banking. Using a recontextualised version of the COM-B (capability, opportunity, motivation – behaviour) model of behaviour change, nudges were deployed in three versions of a fictitious online banking website. Following this, 15 semi-structured interviews were conducted with online banking users from the United States of America to understand how a third party may behave and rationalise their choices when they have unauthorised access to a customer's online banking credentials. The transcripts of these interviews were analysed using thematic analysis. The findings revealed that the most dissuasive nudges focused on encouraging individuals to empathise with the account holder. Nudges that increased the perception of an online banking website's security were also particularly dissuasive. The findings also indicated that the most effective place to deploy these nudges was after a user had logged in. Several rationalisations that enabled individuals to commit online banking fraud were found. The three most common were crime of opportunity, down on their luck, and sunk cost fallacy and curiosity. Together, the findings provide evidence to suggest that, if used effectively, nudges could prove useful as a means of dissuading online banking fraud, and even more so when combined with traditional cybersecurity measures.

DECLARATION

I, Takudzwa Mutyavaviri, hereby declare that:

- the work in this thesis is my own work;
- all sources used or referred to have been documented and recognised;
- this thesis has not previously been submitted in full or partial fulfilment of the requirements for a qualification; and
- I am fully aware of Rhodes University's plagiarism policy and have taken every precaution to comply with the regulation.

1 December 2022

Date

ACKNOWLEDGEMENTS

Beyond the feedback and guidance provided by my supervisors, Dr Van der Schyff and Prof. Renaud, I would like to acknowledge the NRF funding allocated to help recruit participants for this study. I would also like to acknowledge my mother for her emotional and financial support throughout my years at Rhodes University.

GLOSSARY

| | |
|----------------------|--|
| Account holder | The bank's client who uses an online banking service. |
| Third party | An individual who is neither the account holder nor a representative of the bank, who happens to stumble upon compromised credentials or an open (logged-in) account of a customer. |
| Traditional security | Pre-existing cybersecurity measures that are employed by banks to protect their clients and online banking service. |
| User | The individual accessing the website and online banking account. The only user authorised to access an online banking account and its related functionality should be the account holder. |
| Online banking fraud | Transactions and account changes performed by an unauthorised user of an online banking account (i.e., a third party). |
| Choice architecture | The context or environment in which a decision is made. For an online banking website, this is the website's user interface. |
| Choice architect | The individual or organisation responsible for designing or altering the choice architecture. In this context, the bank and their website development team (or service provider). |
| Nudging | <p>A behavioural intervention that uses deliberate choice architecture manipulation(s):</p> <ul style="list-style-type: none"> • to alter an individual's behaviour in a predictable way, • without blocking any of the individual's alternatives/options, • or significantly changing their economic incentives. |

TABLE OF CONTENTS

| | |
|----------------------------|------|
| ABSTRACT | i |
| DECLARATION..... | ii |
| ACKNOWLEDGEMENTS | iii |
| GLOSSARY | iv |
| LIST OF FIGURES..... | xi |
| LIST OF TABLES | xv |
| LIST OF ABBREVIATIONS..... | xvii |

CHAPTER 1: INTRODUCTION AND OVERVIEW

| | | |
|-----|---|---|
| 1.1 | Introduction | 1 |
| 1.2 | Problem Description..... | 3 |
| 1.3 | Goals of Research | 4 |
| 1.4 | Research Questions | 4 |
| 1.5 | Methods, Procedures, and Techniques | 4 |
| 1.6 | Contribution | 5 |
| 1.7 | Ethical Considerations | 6 |
| 1.8 | Thesis Structure..... | 6 |

CHAPTER 2: ONLINE BANKING AND SECURITY

| | | |
|-----|---------------------------|----|
| 2.1 | Introduction | 7 |
| 2.2 | Online Banking..... | 7 |
| 2.3 | Threats and Security..... | 10 |
| 2.4 | Why Behavioural?..... | 14 |
| 2.5 | Summary | 16 |

CHAPTER 3: (DIS)HONESTY, BEHAVIOUR, AND RATIONALISATIONS

| | | |
|-----|-------------------------------------|----|
| 3.1 | Introduction | 17 |
| 3.2 | COM-B Model | 17 |
| 3.3 | Dual Process Model..... | 20 |
| 3.4 | The Traditional Economic Model..... | 21 |
| 3.5 | Rationalisation and Dishonesty..... | 21 |
| 3.6 | (Dis)honest Behaviour | 25 |
| 3.7 | Summary | 30 |

CHAPTER 4: NUDGING

| | | |
|---------|---|----|
| 4.1 | Introduction | 31 |
| 4.2 | Nudging | 31 |
| 4.3 | Nudging Techniques and Interventions..... | 35 |
| 4.3.1 | Decision Information..... | 38 |
| 4.3.1.1 | <i>Translate Information</i> | 38 |
| 4.3.1.2 | <i>Increase the Salience of Information</i> | 39 |
| 4.3.1.3 | <i>Make Information Visible</i> | 39 |
| 4.3.1.4 | <i>Phrasing of Information</i> | 39 |
| 4.3.2 | Decision Structure | 40 |
| 4.3.2.1 | <i>Change Defaults</i> | 41 |
| 4.3.2.2 | <i>Change Option-Related Effort</i> | 41 |
| 4.3.2.3 | <i>Change Range or Composition of Options</i> | 41 |
| 4.3.2.4 | <i>Change Option Consequences</i> | 42 |
| 4.3.3 | Decision Assistance | 42 |
| 4.3.3.1 | <i>Provide Reminders</i> | 43 |
| 4.3.3.2 | <i>Facilitate Commitment</i> | 43 |
| 4.3.4 | Social Decision Appeal..... | 44 |

| | | |
|---------|---|----|
| 4.3.4.1 | <i>Increase Reputation of Messenger</i> | 45 |
| 4.3.4.2 | <i>Provide Social Reference Point</i> | 45 |
| 4.3.4.3 | <i>Instigate Empathy</i> | 45 |
| 4.4 | Summary | 52 |

CHAPTER 5: METHODOLOGICAL APPROACH

| | | |
|---------|--|----|
| 5.1 | Introduction | 53 |
| 5.2 | Research Paradigm | 53 |
| 5.3 | Approach to Theory Development | 54 |
| 5.4 | Research Strategy | 54 |
| 5.5 | Data Collection and Analysis | 56 |
| 5.5.1 | Secondary Data | 56 |
| 5.5.2 | Primary Data | 57 |
| 5.5.2.1 | <i>Participants</i> | 58 |
| 5.5.2.2 | <i>Data Collection: Semi-Structured Interviews</i> | 60 |
| 5.5.3 | Instrument Design | 64 |
| 5.5.4 | Data Analysis | 69 |
| 5.6 | Summary | 72 |

CHAPTER 6: FINDINGS AND ANALYSIS

| | | |
|-------|--|----|
| 6.1 | Introduction | 73 |
| 6.2 | Sample Demographics | 73 |
| 6.3 | Most Effective Nudges | 74 |
| 6.3.1 | PRE-LOG Version | 75 |
| 6.3.2 | POST-LOG Version | 77 |
| 6.3.3 | Across All Three Versions | 78 |
| 6.4 | PRE-LOG vs POST-LOG Effectiveness Comparison | 79 |

| | | |
|--------|--|-----|
| 6.4.1 | Overall Impression of More Likely Behaviour(s)..... | 80 |
| 6.4.2 | Comparisons of the PRE-LOG and POST-LOG Versions..... | 83 |
| 6.5 | Participant Rationalisations..... | 85 |
| 6.5.1 | Hurt Them Because of Their Mistakes | 93 |
| 6.5.2 | Digital Context and Perception of Risk..... | 93 |
| 6.5.3 | Possible Opportunity to Enrich Self..... | 95 |
| 6.5.4 | Legal Restrictions + Moral and Social Norms..... | 97 |
| 6.5.5 | Moral Self-Concept Threat | 99 |
| 6.5.6 | People's Inherent Nature Dictates Their Response to Opportunity/Scenario..... | 99 |
| 6.5.7 | Justify Explaining Fraud Opportunity with Biased Logic..... | 101 |
| 6.5.8 | Harming a Real Person Is Much Harder..... | 103 |
| 6.5.9 | Opportunism and Justification in the Digital Context | 105 |
| 6.5.10 | Empathy and Personalisation..... | 106 |
| 6.5.11 | Laws and Social Norms..... | 106 |
| 6.6 | Summary | 107 |

CHAPTER 7: DISCUSSION

| | | |
|---------|--------------------------------------|-----|
| 7.1 | Introduction | 109 |
| 7.2 | Goals of the Research Revisited..... | 109 |
| 7.3 | Effective Nudges..... | 109 |
| 7.4 | Deployment of Nudges | 112 |
| 7.5 | Rationalisations..... | 115 |
| 7.5.1 | Laws, Morals, and Social Norms | 115 |
| 7.5.1.1 | <i>Help Fellow Man</i> | 115 |
| 7.5.1.2 | <i>Threat of Punishment</i> | 116 |
| 7.5.2 | Empathy and Personalisation..... | 117 |

| | | |
|---|---|-----|
| 7.5.3 | Opportunism and Justification in the Digital Context | 119 |
| 7.5.3.1 | <i>Digital Context and Risk</i> | 119 |
| 7.5.3.2 | <i>Justification-Biased Logic</i> | 120 |
| 7.6 | Summary | 125 |
| CHAPTER 8: CONCLUSION | | |
| 8.1 | Introduction | 126 |
| 8.2 | Problem Description Revisited | 126 |
| 8.3 | Research Questions Revisited..... | 127 |
| 8.3.1 | RQ1: Which choice architecture manipulations (“nudges”) are the most effective at dissuading online banking fraud?..... | 127 |
| 8.3.2 | RQ2: When comparing the placement of nudges before and after logging in, where is it more effective to deploy nudging to dissuade online banking fraud? | 127 |
| 8.3.3 | RQ3: If a third party impersonates or defrauds the legitimate account holder, how do these individuals rationalise their dishonest actions? | 128 |
| 8.4 | Methodological Approach Used | 128 |
| 8.5 | Research Contribution | 129 |
| 8.6 | Implications for Theory..... | 129 |
| 8.7 | Implications for Practice | 130 |
| 8.8 | Limitations and Future Research | 130 |
| 8.9 | Summary of the Thesis | 132 |
| REFERENCES | | 133 |
| APPENDICES | | |
| APPENDIX A: NUDGE MECHANISMS AND COM-B FACTOR MAPPING | | 154 |
| APPENDIX B: INTERFACES AND NUDGES | | 179 |

| | |
|--------------------------------------|-----|
| APPENDIX C: INTERVIEW QUESTIONS..... | 212 |
| APPENDIX D: MAPS | 217 |
| APPENDIX E: MISCELLANEOUS | 239 |

LIST OF FIGURES

| | | |
|-------------|---|----|
| Figure 3.1: | The “simple” COM-B model..... | 19 |
| Figure 3.2: | The “comprehensive” COM-B model of behaviour change | 19 |
| Figure 3.3: | Dishonesty conceptualised as a three-dimensional construct..... | 26 |
| Figure 4.1: | Taxonomy of nudging mechanisms..... | 37 |
| Figure 4.2: | Decision information nudges | 38 |
| Figure 4.3: | Decision structure nudges..... | 40 |
| Figure 4.4: | Decision assistance nudges..... | 43 |
| Figure 4.5: | Social decision appeal nudges..... | 44 |
| Figure 5.1: | Control homepage screenshot | 65 |
| Figure 5.2: | PRE-LOG homepage top | 66 |
| Figure 5.3: | PRE-LOG homepage bottom | 67 |
| Figure 5.4: | Interaction DISABLED screenshot cropped | 68 |
| Figure 5.5: | Interaction DISABLED: Full page | 69 |
| Figure 5.6: | An initial thematic map for the PRE-LOG version rationalisations..... | 70 |
| Figure 5.7: | A refined thematic map for the PRE-LOG version rationalisations..... | 71 |
| Figure 6.1: | PRE-LOG version SIGNIFICANT nudges mind map | 75 |
| Figure 6.2: | POST-LOG version SIGNIFICANT nudges mind map | 77 |
| Figure 6.3: | General SIGNIFICANT nudges mind map | 79 |
| Figure 6.4: | Behaviour of hypothetical third parties in the scenario(s)..... | 82 |
| Figure 6.5: | Comparison and combination of PRE-LOG and POST-LOG | 84 |
| Figure 6.6: | Initial thematic map POST-LOG thought process and rationalisations extract (Phase 3)..... | 87 |
| Figure 6.7: | Initial thematic map POST-LOG thought process and rationalisations (no quotations version) (Phase 3) | 88 |

| | |
|--|-----|
| Figure 6.8: POST-LOG thought process and rationalisations refined V1 (Phase 4) | 89 |
| Figure 6.9: POST-LOG thought process and rationalisations refined V2 (Phase 4) | 90 |
| Figure 6.10: POST-LOG thought process and rationalisations refined V3 (Phase 4) | 91 |
| Figure 6.11: Rationalisations thematic map derived from all three versions (Phase 4 product)..... | 92 |
| Figure 6.12: Rationalisations final thematic map (Phase 5 product) | 105 |
| Figure A1: Taxonomy of nudging mechanisms..... | 154 |
| Figure A2: Decision information nudges | 156 |
| Figure A3: Decision structure nudges..... | 166 |
| Figure A4: Decision assistance nudges..... | 171 |
| Figure A5: Social decision appeal nudges..... | 175 |
| Figure B1: Control and POST-LOG homepage | 179 |
| Figure B2: Control and PRE-LOG summary page..... | 180 |
| Figure B3: Control and PRE-LOG transaction history (page 1) | 181 |
| Figure B4: Control and PRE-LOG transaction history (page 2) | 182 |
| Figure B5: Control and PRE-LOG transaction history (page 3) | 183 |
| Figure B6: Control and PRE-LOG payments page | 184 |
| Figure B7: Control and PRE-LOG add recipients form | 185 |
| Figure B8: Control and PRE-LOG pay recipient page | 186 |
| Figure B9: Control and PRE-LOG internal transfers..... | 187 |
| Figure B10: PRE-LOG homepage top | 188 |
| Figure B11: PRE-LOG homepage bottom | 189 |
| Figure B12: POST-LOG summary page..... | 190 |
| Figure B13: POST-LOG transaction history (page 1) | 191 |

| | |
|--|-----|
| Figure B14: POST-LOG transaction history (page 2) | 192 |
| Figure B15: POST-LOG transaction history (page 3) | 193 |
| Figure B16: POST-LOG payments page | 194 |
| Figure B17: POST-LOG add recipients form | 195 |
| Figure B18: POST-LOG pay recipient form | 196 |
| Figure B19: POST-LOG payment processing..... | 197 |
| Figure B20: POST-LOG payments confirmation page..... | 198 |
| Figure D1: Thought process and rationalisations (Control) project map (Phase 2 of Braun and Clarke, 2006) | 217 |
| Figure D2: Initial thematic map (Control) thought process and rationalisations: left side (Phase 3) | 218 |
| Figure D3: Initial thematic map (Control) thought process and rationalisations: right side (Phase 3) | 219 |
| Figure D4: Initial thematic map (Control) thought process and rationalisations (no quotations: Phase 3 product) | 220 |
| Figure D5: Control thought process and rationalisations refined V1 (Phase 4)... | 221 |
| Figure D6: Control thought process and rationalisations refined V2 (Phase 4)... | 222 |
| Figure D7: Control thought process and rationalisations refined V3 (Phase 4)... | 223 |
| Figure D8: PRE-LOG thought process and rationalisations project map (Phase 2 of Braun and Clarke, 2006)..... | 224 |
| Figure D9: Initial thematic map: PRE-LOG thought process and rationalisations: left side (Phase 3) | 225 |
| Figure D10: Initial thematic map: PRE-LOG thought process and rationalisations: right side (Phase 3) | 226 |
| Figure D11: Initial thematic map: PRE-LOG thought process and rationalisations (no quotations) (Phase 3)..... | 227 |
| Figure D12: PRE-LOG thought process and rationalisations refined V1 (Phase 4) | 229 |

| | |
|--|-----|
| Figure D13: PRE-LOG thought process and rationalisations refined V2 (Phase 4) | 230 |
| Figure D14: PRE-LOG thought process and rationalisations refined V3 (Phase 4) | 231 |
| Figure D15: POST-LOG thought process and rationalisations project map (Phase 2 of Braun and Clarke, 2006)..... | 232 |
| Figure D16: Initial thematic map POST-LOG thought process and rationalisations: left side (Phase 3) | 233 |
| Figure D17: Initial thematic map POST-LOG thought process and rationalisations: right side (Phase 3) | 234 |
| Figure D18: Initial thematic map (POST-LOG) thought process and rationalisations: no quotations (Phase 3 product) | 235 |
| Figure D19: POST-LOG thought process and rationalisations refined V1 (Phase 4) | 236 |
| Figure D20: POST-LOG thought process and rationalisations refined V2 (Phase 4) | 237 |
| Figure D21: POST-LOG thought process and rationalisations refined V3 (Phase 4) | 238 |
| Figure E1: Entity Relationships Diagram (ERD) of limited online banking system..... | 239 |
| Figure E2: Behavioural state machine: Login | 240 |
| Figure E3: Behavioural state machine: Payment..... | 241 |
| Figure E4: Hierarchical task analysis (HTA): Online banking website | 242 |
| Figure E5: HTA: Access services (payments) | 243 |

LIST OF TABLES

| | | |
|------------|---|-----|
| Table 2.1: | The various threats linked to online banking | 10 |
| Table 2.2: | Known traditional security measures that banks can employ to help secure online banking | 12 |
| Table 2.3: | Threat and corresponding traditional response | 14 |
| Table 3.1: | A summary of the findings regarding honesty | 29 |
| Table 4.1: | The five behavioural interventions..... | 35 |
| Table 4.2: | Nudges and COM-B factors | 47 |
| Table 5.1: | Example of keywords used | 57 |
| Table 5.2: | Interview guide (Control version)..... | 62 |
| Table 5.3: | Interview guide (PRE-LOG version)..... | 62 |
| Table 5.4: | Interview guide (POST-LOG version)..... | 63 |
| Table 5.5: | Interview guide (comparison of versions)..... | 63 |
| Table 6.1: | Sample demographics (n=15) | 74 |
| Table 6.2: | POST-LOG rationalisation refinement 1 | 89 |
| Table 6.3: | POST-LOG rationalisation refinement 2..... | 90 |
| Table 6.4: | POST-LOG rationalisation refinement 3..... | 91 |
| Table 7.1: | Rationalisations ranked | 125 |
| Table B1: | POST-LOG nudges | 199 |
| Table B2: | PRE-LOG nudges | 207 |
| Table D1: | Control rationalisation refinement 1 | 220 |
| Table D2: | Control rationalisation refinement 2..... | 221 |
| Table D3: | Control rationalisation refinement 3..... | 222 |
| Table D4: | PRE-LOG rationalisation refinement 1 | 228 |
| Table D5: | PRE-LOG rationalisation refinement 2 | 229 |
| Table D6: | PRE-LOG rationalisation refinement 3 | 230 |

| | | |
|-----------|---|-----|
| Table D7: | POST-LOG rationalisation refinement 1 | 235 |
| Table D8: | POST-LOG rationalisation refinement 2 | 236 |
| Table D9: | POST-LOG rationalisation refinement 3 | 237 |

LIST OF ABBREVIATIONS

| | |
|----------|---|
| 2FA | Two-factor authentication |
| ATM | Automated teller machine |
| COM-B | Capability, opportunity, motivation – behaviour [model] |
| ERD | Entity Relationships Diagram |
| F.O.B.T. | Fear of being tracked |
| HIT | Human Intelligence Task |
| HTA | Hierarchical Task Analysis |
| ID | Identification |
| IDPS | Intrusion Detection and Prevention Systems |
| MIME | Multipurpose Internet Mail Extension |
| MTurk | Mechanical Turk |
| OTP | One-time password |
| PIN | Personal identification number |
| RU-HREC | Rhodes University Human Research Ethics Committee |
| SMS | Short Message Service |
| SSL | Secure Socket Layer |
| TMS | Transaction monitoring system |
| UI | User interface |
| URL | Uniform Resource Locator |
| USA | United States of America |
| USB | Universal Serial Bus |

CHAPTER 1:

INTRODUCTION AND OVERVIEW

1.1 Introduction

Online banking (also referred to as Internet banking) has existed for several decades and has become a standard and popular feature of modern banking (Sarreal, 2019; Pilcher, 2020). Such popularity has been fuelled by the ease with which clients can access and manage their accounts and the remote nature of such activities (i.e., there is less need to go to the bank in person). Most banking services require account holders (users) to authenticate themselves using their login credentials to access online banking. These credentials must be kept secure to prevent impersonation (Gupta, 2006; Singh, 2020). If impersonated (correct credentials used by an unauthorised user), the potential financial loss can be devastating to the legitimate account holder when impersonators commit online banking fraud. According to the South African Banking Risk Information Centre (2020:19), the gross financial loss from online banking fraud in 2019 was R147 000 000, with 3027 incidents of online banking fraud that year. The average financial loss per incident was R48 589. Whilst all these incidents may not have dealt with compromised, the financial impact on banks and their clients was significant overall. In the context of the United States of America (USA), online banking can account for up to 33% of the costs their banks incur as a result of fraud (American Banking Association, 2022; Dang, 2022). Beyond the significant financial loss of being a victim of online banking fraud, such incidents also frustrate American citizens and damage the trust they place in their banks, which subsequently impacts the bank's ability to attract new clients or retain existing ones (Hoffmann and Birnbrich, 2012). To help avoid such incidents, it is essential that clients keep their online banking credentials safe.

Security advice regarding credentials may be readily available, but users still exhibit negligent behaviour (Gehring, 2002; Stobert, 2014; Stobert and Biddle, 2014; Sanchez, 2019). Such negligent behaviour includes failing to log out, saving credentials on a public machine, or insecurely storing written credentials. As a result, the user's account has a higher chance of becoming compromised, i.e., falling into the hands of third parties. In this study, third parties are defined as any other individual not

involved in the direct relationship between the bank and its online clients (Kenton, 2020; *Collins English Dictionary*, 2021). With credentials in hand, third parties can gain unauthorised access to the online banking account, impersonate the legitimate account holder, and commit fraud if so desired. Such fraudulent activity is difficult to detect using traditional security mechanisms as third parties can pass the authentication check(s) used on the website, i.e., log in normally (Wei et al., 2013). As a result, they gain virtually unrestricted access as the online banking system treats them as legitimate account holders. This leaves the legitimate account holder with very little they can do at that moment to protect their funds from the third party impersonating them.

Although virtually all online banking websites in North America make use of credentials to access online accounts, only some of them also use two-factor authentication (2FA) to prevent unauthorised logins (Aguiler, 2015; Colbert, 2019). 2FA is an authentication system that requires a second code or personal identification number (PIN) beyond the account holder's credentials to log in successfully (Bursztein et al., 2014; Colbert, 2019; Eddy, 2019). Those banks that do not to implement 2FA normally cite concerns about reducing online banking' convenience due to the additional hassles their clients will face accessing their accounts (French, 2012; Global Message Services, 2021). Some clients decide to opt out of using 2FA due to accessibility issues such as visual impairment or dyslexia, while others opt out due to lack of access to a second device or email to receive the code (Renaud, Johnson and Ophoff, 2020; Renaud, 2021). Putting aside the issues of accessibility and convenience, traditional security measures may prove insufficient because, in any security system, humans can be a major weak point (Mouton et al., 2014; Mouton, Leenen and Venter, 2016). This is because people can unintentionally be manipulated to reveal sensitive information or compromise the system's security (Mouton et al., 2014; Mouton et al., 2016).

To address the issues listed thus far and improve security for those who cannot use 2FA PINs, banks can potentially employ nudging. That is what this study aimed to research. Nudges are choice architecture manipulations designed to subtly influence an individual's behaviour – in this case, the third party – towards the decision the choice architect wants (Thaler and Sunstein, 2008; Renaud and Zimmermann, 2018). Considering that the third party can still decide not to commit fraud after logging in, the nudges employed, in this case, aim to persuade them to log out, leaving the account

holder's funds intact. The choice architecture within the context of an online banking website refers to the website layout, the interaction design, information presentation, how it appears to the client, as well as the resultant choices made when a client transacts online (Thaler and Sunstein, 2008; Franco, 2018).

Nudging has been employed in a variety of other offline contexts, including encouraging healthier eating habits (Kroese, Machiori and De Ridder, 2015; Broers et al., 2017), convincing farmers to adopt more environmentally friendly practices (Kuhfuss et al., 2016), and encouraging college attendance among teens from lower-income backgrounds (Castleman and Page, 2015). It has been applied in various online or digital contexts, such as online user recommendation systems (Jesse and Jannach, 2021), social networks, and privacy decisions (Kroll and Stieglitz, 2021). Nudging has already been applied in the context of online banking to some degree. It has been used to boost customer retention and encourage wiser savings decisions (Akther and Tariq, 2022; Costa, 2022), and to boost youth engagement with banking applications (Wijland, Hansen and Gardezi, 2016). This study investigated the use of nudging to combat online banking fraud – a novel approach within this context.

1.2 Problem Description

Banking institutions stress the importance of keeping online banking credentials secure. Unfortunately, many clients cannot memorise their credentials and thus engage in coping strategies, such as writing them down, to ensure they can access their accounts when needed (Gehring, 2016; Melissa Sanchez, 2019; Stobert, 2014; Stobert and Biddle, 2014). These client credential coping strategies increase the chances of their credentials being compromised (i.e., falling into the hands of third parties). Given that online banking websites are unable to distinguish between the login of a legitimate account holder as opposed to a third party using compromised credentials, said third party has the opportunity to commit fraud, i.e., steal the account holder's money (Wei et al., 2013). Such unauthorised transactions can result in significant financial loss for banks and their clients.

1.3 Goals of Research

The study had three goals. The first goal was to investigate how effective various nudges were in making it difficult for someone to rationalise committing online banking fraud, and subsequently reveal which nudges would be best able to dissuade instances of online banking fraud. The second goal was focused on where it is ideal to deploy nudges to give the best chance of dissuading online banking fraud. The final goal was to explore and discover some of the rationalisations that individuals may use to commit online banking fraud.

1.4 Research Questions

This study sought to address the following research questions:

- RQ1: Which choice architecture manipulations (“nudges”) are the most effective at dissuading online banking fraud?
- RQ2: When comparing the placement of nudges before and after logging in, where is it more effective to deploy nudging to dissuade online banking fraud?
- RQ3: If a third party impersonates or defrauds the legitimate account holder, how do these individuals rationalise their dishonest actions?

1.5 Methods, Procedures, and Techniques

This study employed a qualitative methodological approach using the interpretivist research paradigm and a (quasi-) experimental research strategy. The COM-B model of behaviour change was utilised to situate the study within theory. According to the COM-B model, behaviour (B) has three precursors: capability (C), opportunity (O), and motivation (M). Any intervention designed to change an individual’s behaviour must target and alter at least one of the three precursors (Mayne, 2016; West and Michie, 2020).

Three versions of an online banking website belonging to the fictional Horizon Banking were developed for this study using the software tool Axure RP. These website(s) were based on several South African and American banks' existing online banking interfaces (choice architecture). The first version, the Control, was the website with no nudges employed anywhere on the interface. The second version, the PRE-LOG,

focused on nudging the individual at the first step, namely logging in. POST-LOG was the final version; it focused on applying nudges to the website after the account had already been logged into.

Data were collected from participants of various age groups through semi-structured virtual interviews. The sample of 15 individuals was gathered using convenience sampling. The virtual interviews were conducted via the video-conferencing software Zoom. During the interviews, the participants were given the opportunity to interact with all three versions of the fictitious online banking website. These interactions were facilitated by the Zoom feature “Give remote control”. As participants interacted with the website, they were asked to envision certain scenarios. These scenarios are further described later in the interview guide in Chapter 5.

The participants were asked to place themselves in the position of the third party with the compromised credentials in the scenario. The interview questions focused on exploring how participants believed third parties in the scenario might behave and rationalise their behaviour. The goal was to help minimise the risk of receiving socially desirable answers by helping them dissociate and imagine another person in the prescribed scenarios. After conducting the interviews, the recordings of the sessions were transcribed and analysed using the thematic analysis process devised by Braun and Clarke (2006). On all versions of the website, the participants’ interactions with the website(s) were observed and recorded. These interaction recordings were used to supplement the thematic analysis of the transcripts.

1.6 Contribution

This study extends the body of knowledge surrounding the behavioural use of nudging and its potential applications in various contexts – in particular, dissuading online banking fraud, which is a previously unexplored application within the cybersecurity field. This study also demonstrates how one could use the COM-B model of behaviour change to theoretically frame the application of said nudging theory and related choice architecture manipulations. The final contribution is to the existing body of literature, as it helps to expand the understanding of how honesty could be encouraged in individuals via choice architecture manipulations. Several rationalisations that either

dissuade or enable fraud were discovered, although some were more prevalent than others.

1.7 Ethical Considerations

Due to the collection of primary data from human participants, ethical approval was sought from the Rhodes University Human Research Ethics Committee (RU-HREC). Approval was granted by the RU-HREC (approval number 2022-5353-6499). The data gathered from the participants (including the website interactions) were anonymised before the analysis began. The three fictitious online banking websites were hosted locally. As such, they were not indexed by any search engine, which rendered them inaccessible to non-participants.

1.8 Thesis Structure

This thesis consists of eight main chapters and appendices. The eight chapters are this introductory chapter, three literature review chapters, the methodology chapter, the findings chapter, the discussion chapter, and the concluding chapter.

CHAPTER 2:

ONLINE BANKING AND SECURITY

2.1 Introduction

The previous chapter focused on introducing the research topic and providing an overview of the study. This chapter is the first of three literature review chapters. It focuses on online banking and security. The subsequent literature review chapter focuses on dishonesty and rationalisations, while the final literature review chapter examines literature related to the concept of nudging and its application in digital contexts.

Online banking has existed for several years (Choubey and Choubey, 2013). Over time, it has become a common service that banks offer (Mannan and Van Oorschot, 2007; Ruiz, Winter and Amatte, 2017). One of the major concerns regarding online banking is its security (Mannan and Van Oorschot, 2007; Yazdanifard et al., 2011). Although banks have invested significant resources into protecting their clients and their funds, online fraud still occurs (Cassim, 2010; More, Jadhav and Nalawade, 2015; Mabunda, 2019). This chapter shows the traditional security measures employed by banks and how some threats to online banking can circumvent them. To help handle such threats, this study proposes incorporating the behavioural intervention of nudging to supplement traditional security. (For more information about how papers were selected for inclusion in the literature review, see Chapter 5.5.1)

2.2 Online Banking

Broadly speaking, e-banking refers to the provision of banking services to clients through electronic channels, including automated teller machines (ATMs), mobile banking, electronic funds transfer, automatic bill payments, telephone transacting, and online banking (Koskosas, 2011; Yazdanifard et al., 2011). Online banking, also known as Internet banking, is a service that most modern banks offer that allows clients to access their accounts and other banking services via the Internet on their computer or smartphone (Osunmuyiwa, 2013; Dzomira, 2014). This study, however focuses more on online banking in the context of being accessed from a browser on a

personal computer, as the mobile phones being easier to steal the device itself or conceal it from others due to their smaller size would have had a significant impact the study's experiment design (the physical opportunity COM-B factor in the scenarios. See Chapter 3.2). Online banking is also linked to e-commerce and online transactions, which have become commonplace in modern times (Syniavska et al., 2019). Although initially thought of as a threat that would replace “traditional” banking, online banking has become an extension of the banking services offered to clients (Omariba, Masese and Wanyembi, 2012). There are various reasons for the growth and popularity of online banking among banks and their clients.

For the banks, the adoption or implementation of online banking has been primarily driven by the potential for increased customer reach and operation cost savings (Williamson, 2006; Mannan and Van Oorschot, 2007; Lee, 2009; Yazdanifard et al., 2011; Bahl, 2012; Usman and Shah, 2013). In terms of increased reach, this is possible through the remote nature of online banking. After signing up for online banking services, a customer needs a device with a browser, an Internet connection, and the correct website URL (Cristina, Beatrice and Florentina, 2008). Nowadays, smartphones and other Internet browsing devices are relatively common (Smith, 2012; Heimerl et al., 2015; Verkijika, 2018). As a result, banks can offer their services to far more clients than “traditional” banking, which relies heavily on “pen and paper” and physical branches. Fewer physical branches, and subsequently less staff, are part of the potential cost savings that banks could experience by promoting online banking (Williamson, 2006; Cristina et al., 2008). The other cost savings come from more efficient and cost-effective transaction processing (Koskosas, 2011). Combining the two helps to reduce the banks' overall operation costs, which allow online banking to increase the bank's profits (Lee, 2009). When implementing changes to their online banking, the impact on customer convenience is a major consideration (Claessens et al., 2002).

For the banks' clients, online banking has various advantages that may draw people towards online banking. Overall, these can be combined into the broader draw of convenience. This convenience is the major draw for clients when deciding to sign up for online banking (Giles, 2010; Omariba et al., 2012). The remote nature of online banking allows clients to access their banking services from anywhere or at any time (Lee, 2009; Belás et al., 2016; Hartl and Schmuntzsch, 2016). Provided they have a

device with an Internet connection and a browser, they do not need to be restricted by bank branch location or operating times. This does not necessarily mean that branches are obsolete, as some services and queries may require in-person visits to the bank (Natter, 2019). Online banking can also potentially provide other advantages, such as faster transaction speeds, lower transaction costs, and supporting online shopping and other e-commerce (Lee, 2009).

While online banking may offer various advantages for clients and banks, it is not without its disadvantages and risks. For the banks, these can include high initial investment, the potential impact on customer relationship building with less in-person contact, finding staff or service providers with necessary technical expertise, and complying with legislation and regulations (Cristina et al., 2008; Bahl, 2012; Osunmuyiwa, 2013; Dzomira, 2014; Belás et al., 2016; Gabudeanu et al., 2021). For the clients, disadvantages include lack of tech literacy, a less personal relationship with the bank, Internet connectivity requirement, service and technical interruptions (i.e., outages), limited services offered, and the privacy of their data (Belás, Korauš and Gabčová, 2015; Natter, 2019; North, 2020).

Online banking security is a major concern for banks and their clients (Nilsson, Adams and Herd, 2005; French, 2012; Belás et al., 2016). Compromised online banking accounts can be used to commit online banking fraud, as transactions and changes can be processed without the account holder's consent (Raghavana and Parthiban, 2014; Shah et al., 2019; Syniavska et al., 2019). The increasing popularity and use of online banking have been accompanied by increased incidents of online banking fraud and cybersecurity incidents (Hisamatsu, Pishva and Nishantha, 2010; Hartl and Schmuntzsch, 2016). For clients, big or small, their concerns are mainly about losing funds due to fraud or losing access to their accounts (French, 2012; Raghavana and Parthiban, 2014; Onaolapo, Mariconti and Stringhini, 2016). The financial impact of online banking fraud having previously been mentioned in Chapter 1.1.

For the banks, security concerns are also tied to the loss of funds and a negative impact on their reputation and clients' trust (Yazdanifard et al., 2011; Hoffmann and Birnbrich, 2012). The trust between the bank and its clients is a component of the broader banking system, as people trust that their funds are secure with the banks they use (Hoffmann and Birnbrich, 2012; Belás et al., 2016). Damage to reputation

and trust can make it harder for the bank to convince potential clients to bank with them. At the same time, security incidents regarding online banking make it more difficult for banks to persuade their clients to adopt online banking (Lee, 2009; Usman and Shah, 2013). There is thus a potential long-term impact beyond financial loss when cybersecurity incidents occur and become public. As a result, communication regarding security measures is essential for how banks (should) market a service like online banking to allay customer fears (Koskosas, 2011). Online fraud's direct or immediate financial losses can still be substantial for banks (Usman and Shah, 2013; Kawugana and Faruna, 2018). According to Clark (2021), the losses from online banking fraud in the United Kingdom alone were approximately £159.7 billion in 2020. To help combat these incidences of fraud, banks invest significant amounts of funds into securing their systems and preventing online banking fraud (Yazdanifard et al., 2011; Raghavana and Parthiban, 2014).

2.3 Threats and Security

The funds that banks invest in their security aim to prevent a variety of threats. Online banking faces several potential threats. Table 2.1 summarises the threats to online banking.

Table 2.1: The various threats linked to online banking

| Threat | Description |
|---------------------------|---|
| Trojan (malware) | Malware disguised as or hidden in the code of another program or file (Dzomira, 2014). |
| Worms (malware) | Malware (software) programs are designed to replicate without any user input and steal data (More et al., 2015). |
| Keyloggers (malware) | Malware that records keystrokes used on individuals' keyboards (Botacin, Kalysch and Grégio, 2019). |
| Viruses (malware) | A software program designed to self-replicate and steal user data (Kraemer-Mbula, Tang and Rush, 2013; Onaolapo et al., 2016). |
| Phishing | Misleading clients usually with false websites, applications, or requests to trick them into revealing sensitive information such as credentials and credit card information (Onaolapo et al., 2016). |
| Pharming | Similar to phishing, the main difference is that the customer's Internet connection or browser is redirected to a false website. Sensitive data such as credentials and credit card information can then be harvested (Fatima, 2011). |
| Social engineering | Non-technical method of cybercrime involving the use of deceit and social manipulation to trick users into revealing privileged information such as credentials (Hartl and Schmunzsch, 2016; Mouton et al., 2016). |
| Man-in-the-middle attacks | Interception of traffic between the customer's client machine and the bank's servers (Hisamatsu et al., 2010; Syniavska et al., 2019). |

| | |
|---|---|
| Denial of service | Making the online banking website unavailable to the bank's clients (Cristina et al., 2008). |
| Packet sniffers | Programs designed to scan snippets of data transmitted between the bank's website and the user's machine/device (Omariba et al., 2012). |
| Other browser- or website-related vulnerabilities | Include clickjacking, cross-site scripting, Multipurpose Internet Mail Extension (MIME) sniffing, and cross-site request forgery (Sood and Enbody, 2011; Ahmad et al., 2021). |
| Server bugs/exploits/hacks | Vulnerabilities or direct cyberattacks on banks' servers for their websites (Ahmad et al., 2021). |

The most common type of attack is phishing and its related threats (Shah et al., 2019; Syniavska et al., 2019; South African Banking Risk Information Centre, 2020). Most of these threats centre around gaining access to the customer's data, usually credentials and credit card numbers. Credentials are the proverbial "keys to the kingdom" as they can allow third parties access to online banking accounts if used to impersonate the actual account holder. Credentials and login details are still the most common form of authentication used by online services around the globe (Boothroyd and Chiasson, 2013; Missaoui et al., 2018). Even among online banking websites, they are often the first, if not the only, form of authentication check to control online banking access (Claessens et al., 2002; Choubey and Choubey, 2013).

Being so common online, most users have no problem knowing how to use credentials. However, their ubiquitous use often results in individuals having a portfolio of credentials to manage. Users make use of various coping strategies to manage those (Stobert and Biddle, 2014). Strategies include reusing the same credentials across multiple accounts, writing down credentials, creating weak passwords, using password managers, and saving credentials on their browsers (Boothroyd and Chiasson, 2013; Stobert, 2014). Unfortunately, some of these coping strategies can increase the security risk of credentials falling into the hands of unauthorised third parties and accounts being compromised (Inglesant and Sasse, 2010; Egelman et al., 2011). For example, with the credential reuse coping strategy, a single compromised account can trigger a "domino effect" as third parties can try the same leaked credentials on the user's other online accounts (Missaoui et al., 2018). Written-down credentials that are not securely stored can be stumbled upon by a random third party (Stobert and Biddle, 2014). However, it is worth noting that some individuals may put more effort into securing more critical accounts, like online banking, by creating stronger and more unique passwords for these accounts (Florêncio, Herley and Van Oorschot, 2014a, 2014b; Stobert and Biddle, 2014). Unfortunately, these credentials

are likely harder to remember, which leads people to record them. Not every online banking user does this, which leaves others vulnerable to the risks created by their coping strategies.

Specifically focusing on the credentials, banks may employ different security measures and policies to help manage the risks. These include lockouts, password composition requirements, password length requirements, password expiration, and blacklists (Gehringer, 2002; Florêncio, Herley and Coskun, 2007; Egelman et al., 2011; Florêncio et al., 2014a). Like other online services, banks may also have password rules that forbid users from sharing their credentials, writing them down, or reusing them (Zhang-Kennedy, Chiasson and Van Oorschot, 2016). Unfortunately, the more rules and security measures that are added to credential creation, the more difficult it becomes for users to manage them. The increase in complexity decreases the usability of credentials for users and can affect security as it drives users towards risky coping strategies (Inglesant and Sasse, 2010; Zhang-Kennedy et al., 2016).

Despite providing better security, these credential-related security measures are still limited. Credentials, in general, are vulnerable to different guessing attacks and password cracking, if not just stolen outright through phishing or social engineering (Omariba et al., 2012; Florêncio et al., 2014b; İşler, Küpçü and Coskun, 2019). As a result, some banks move beyond this simple and convenient form of authentication and may employ various other security measures to protect their clients. These security measures can be a combination of hardware and software, but for the most part, are software based (Omariba et al., 2012; Belás et al., 2015). Table 2.2 summarises a few of these security measures.

Table 2.2: Known traditional security measures that banks can employ to help secure online banking

| Security measure | Description |
|---|--|
| Intrusion Detection and Prevention Systems (IDPS) | A system designed to detect intrusions into the bank's network automatically and alert staff (French, 2012; Whitman and Mattord, 2018). |
| Firewalls | Software and/or hardware that filters and prevents specific traffic from an unsafe network/source, i.e., the Internet. It can be employed on the bank's side and/or the end user's device/machine (Omariba et al., 2012; Whitman and Mattord, 2018). |
| 2FA | A form of multi-factor authentication that uses two methods to verify the user's identity. Most commonly in the form of a one-time password (OTP) / PIN, sent to the account holders via SMS, email, or app notification (Saby, 2007; İşler et al., 2019). |

| Security measure | Description |
|--|--|
| Proxy servers | A server that intercepts and handles requests coming from the end users of online banking by retrieving the appropriate resource from the bank's internal servers (French, 2012; Whitman and Mattord, 2018). |
| Data analytics | Analysing user data to detect fraud by spotting anomalies in the transactions and user actions performed in an online banking account (Mannan and Van Oorschot, 2007; Bănărescu, 2015). |
| Encryption | Conversion of sensitive data from plaintext into an unreadable format. Unauthorised individuals should have no way to reverse encryption without the appropriate decryption keys. Used by banks to protect data on their servers (Usman and Shah, 2013; Florêncio et al., 2014a; Whitman and Mattord, 2018). |
| USB tokens | Additional hardware-based authentication. Beyond authenticating using credentials, end users need to connect a USB device to their machine. This USB contains a unique key or identifier and is sometimes used with 2FA (Claessens et al., 2002; Williamson, 2006; Fatima, 2011; Krol et al., 2015). |
| Tokens, smartcards, and card readers | Additional hardware-based authentication (2FA) is plugged into the end user's machine via USB. This launches a browser on the user's machine and establishes a connection that is supposed to be secure. Scanning their card is used to authenticate the user's identity (Giles, 2010). |
| Biometrics | Scanning of customer biometric data, usually fingerprints, to authenticate the end user of online banking. They are typically used as part of multi-factor authentication, ideally as a supplement to 2FA (Fatima, 2011; Belás et al., 2016). |
| Education and awareness programmes | Information-providing/-sharing programmes launched by banks to help improve clients' and/or their own staff's understanding of potential threats and how they can be mitigated (Omariba et al., 2012; Usman and Shah, 2013). |
| Secure Socket Layer (SSL) certificates | SSL is a security measure employed on browsers that encrypts the connection to the website. For the end user, it displays a simple lock icon representing a secure website connection (Hisamatsu et al., 2010; Fatima, 2011; Omariba et al., 2012). |
| Anti-virus and anti-spyware | Pieces of software that banks recommend or sometimes require that end users install on their machines/devices. This software, often provided by other third-party vendors, is designed to scan, detect, and remove malware on the end user's machine (Mannan and Van Oorschot, 2007). |

Table 2.3 summarises the common traditional security measures employed to handle some of the threats faced by online banking. Banks may potentially employ more security measures to protect online banking, especially on their back-end, but the specifics of such measures are often not public knowledge. Giles (2010) criticises the secrecy and lack of cooperation among banks regarding protecting online banking accounts; he argues that this prevents some vulnerabilities from being detected earlier. On the other hand, Li and Luo (2012) argue for secrecy regarding information security as it potentially makes it possible to detect threat actors who inadvertently activate these security measures.

Table 2.3: Threat and corresponding traditional response

| Threat | Corresponding traditional security response |
|--|---|
| Phishing and pharming | Biometrics, tokens, 2FA, education and awareness programmes |
| Malware (trojans, worms, spyware) | Anti-virus, firewalls |
| Browser-based threats | SSL certificates, encryption |
| Packet sniffers, man-in-the-middle attacks | Data analytics, IDPS |
| Social engineering | Education and awareness programmes |
| Server bugs/exploits/hacks | Firewalls, IDPS, encryption, proxy servers |
| Denial of service | IDPS |

2.4 Why Behavioural?

Despite all the funds and security measures that banks employ, online banking fraud still occurs (Ahmad et al., 2021). Cybersecurity, in general, tends to be more reactive, as the pace of innovation in cybercrime outpaces it (Kraemer-Mbula et al., 2013; Lee, 2019). This is partly why no security system, no matter how technologically advanced, will be perfect or completely invulnerable (French, 2012; Enofe et al., 2017). Additionally, the security measures in Table 2.2, while improving security, unfortunately do impose a trade-off regarding usability (Mannan and Van Oorschot, 2007). Generally, when security measures and policies become less usable, people search for workarounds or coping mechanisms (Stobert, 2014; Yevseyeva et al., 2015). The focus on increasing traditional security and the subsequent usability cost also impacts the accessibility of online banking (Renaud, 2021). Lack of accessibility considerations can make it more difficult for online banking users to utilise the security measures on offer. Considering that a significant and growing proportion of the world's population is getting older, accessibility considerations will grow in importance in the future (United Nations Department of Economic and Social Affairs, 2019; Winkie, 2021).

The trade-off in usability often has a negative impact on the convenience of online banking (Krol et al., 2015). This, in turn, can cause frustration for existing online banking users and reduce the allure for the bank's other clients. As a result, security measures employed by the bank need to strike a balance between the security of online banking and its usability (Mannan and Van Oorschot, 2007; Choubey and Choubey, 2013). Some banks may be willing to make the usability trade-off, while others may not. Those that choose not to often keep authentication and security for the user as simple and convenient as possible (Williamson, 2006). This ties into a

broader problem for online banking: security measures are not standardised (Choubey and Choubey, 2013). One bank may therefore only have a login screen and credentials, while another uses multi-factor authentication with OTPs or biometrics. As a result, the level of security offered across various banks and their online services can vary significantly.

Beyond the usability cost that comes with increasingly complex and technical security measures, ignoring security's human and behavioural aspects can also create serious vulnerabilities (Adams and Sasse, 1999; Desisa and Beshah, 2014), especially when it comes to online banking, as threats like keyloggers, social engineering, phishing, and pharming can target the online banking user and their device(s) rather than the banks' secure systems (Moore, Clayton and Anderson, 2009; Desisa and Beshah, 2014; Hartl and Schmuntzsch, 2016). Targeting the human user helps third parties effectively bypass some of the security measures that banks and other organisations may have invested in (More et al., 2015; Mouton et al., 2016). For example, a bank can invest heavily in state-of-the-art IDPS and encryption, only for an attacker to use social engineering to trick their customers into revealing their credentials. With the credentials, the attacker can compromise the online banking account without triggering an IDPS alert. Security measures that incorporate or consider the human or behavioural aspect of information systems could supplement existing technological measures that banks already employ in online banking security.

According to Krol et al. (2015), the ideal authentication system for online banking is fast, simple, and minimises the cognitive and physical effort required on the user's part. Nudging is a behavioural intervention that can potentially accomplish most of these requirements, as it can potentially improve security while imposing a minimal impact on usability (Acquisti, 2009). Nudging, as a behavioural intervention, has been employed in other information security studies and privacy studies. For example, Dolan et al. (2012) employed digital nudging to encourage social network users to be more mindful of the information they reveal online. Choe et al. (2013) and Zhang and Xu (2016) performed similar studies and employed nudging to reduce the chances of people installing privacy-invasive applications on their devices. Turland et al. (2015) and Jeske et al. (2014) conducted similar studies and employed nudging to encourage people to avoid insecure wireless networks. Story et al. (2020) employed nudging to persuade people to switch from point-of-sale machines to more secure mobile

payment options. Petrykina, Schwartz-Chassidim and Toch (2021) employed nudging via a gamified virtual environment to reduce the chances of individuals downloading malicious software. Ioannou et al. (2021) conducted a systematic literature review and concluded that nudging could be employed to alter privacy-related behaviour. Renaud et al. (2017) and Hartwig and Reuter (2021) employed nudging in password security-related studies.

Recognising that there is no perfect security system, no deployed behavioural techniques can replace existing security measures already employed by banks but must rather supplement them. This study explored the potential impact of employing a behavioural intervention such as nudging to dissuade online banking fraud. This is a novel application of nudging, as far as the literature found would suggest. Additionally, the study also sought to determine where it would be ideal to deploy said nudges before or after the user logged in.

2.5 Summary

This chapter focused on online banking security and the potential for behavioural interventions such as nudging. The next chapter focuses on the theory regarding behaviour, (dis)honesty, and rationalisations. Thereafter, Chapter 4 focuses specifically on nudging-related literature.

CHAPTER 3: (DIS)HONESTY, BEHAVIOUR, AND RATIONALISATIONS

3.1 Introduction

The previous chapter considered online banking and the traditional security employed by banks to combat some of the more common threats. This chapter focuses on literature regarding the rationalisations and behaviour of individuals to gain a sense of how honest a hypothetical third party could be expected to behave in various scenarios. It is intrinsically linked to the third research question, as the goal was to explore what had already been written regarding the factors that encourage or justify dishonest behaviour. (For more information about how papers were selected for inclusion in the literature review, see Chapter 5.5.1)

3.2 COM-B Model

Michie, Van Stralen and West (2011) originally proposed the COM-B model as part of a broader behavioural change framework known as the behaviour change wheel¹. This study primarily focused on the COM-B model rather than the whole framework. The COM-B model of behaviour change proposes that for any behaviour to take place, it needs to be preceded by three factors: capability, opportunity, and motivation. Thus, any intervention attempting to alter an individual's behaviour must affect at least one of the three factors (Mayne, 2016; Howlett et al., 2019; Keyworth et al., 2020; West and Michie, 2020). Each of these factors can be split into two subfactors.

Capability refers to an attribute of the individual(s) that allows them to take advantage of an available opportunity. It can be broken down into psychological capability and physical capability (Barker, Atkins and De Lusignan, 2016; West and Michie, 2020). Psychological capability deals with the individual's understanding, memory, and skills that enable them to perform a behaviour. Physical capability refers to the individual's physical capacity to carry out the behaviour in question.

¹ <https://implementationscience.biomedcentral.com/counter/pdf/10.1186/1748-5908-6-42.pdf>

Opportunity refers to an attribute of the external environment that makes it possible for an individual to perform the behaviour in question; it can be broken down into social opportunity and physical opportunity (Barker et al., 2016; West and Michie, 2020). Physical opportunity naturally refers to the aspects of the physical environment in which individuals find themselves. On the other hand, social opportunity involves the culture and norms of the people and organisations around the individual that either encourage or facilitate the behaviour.

Motivation refers to an aggregate of the mental processes that energise and direct an individual's behaviour. It can be broken down into automatic and reflective motivation (Barker et al., 2016; West and Michie, 2020). Automatic motivation involves thought processes tied to instincts, habits, and desires. On the other hand, reflective motivation deals more with a conscious thought process tied to planning and evaluating different options.

At its simplest, the COM-B model describes the relationship(s) between capability, opportunity, and motivation with behaviour. It can, however, be more complicated. The relationship between the three factors and behaviour can be bidirectional; behaviour can thus influence capability, opportunity, and motivation, and vice versa (Michie et al., 2011; Mayne, 2016). For example, consider a sport; an individual can join a certain sports club while they are still in school. Their motivation could be that they were required to play at least one sport, the opportunity being the sport is offered by their school, and their capability being young and fit. As they play the sport, their skills improve, and they may begin to enjoy playing the sport. From the original capability, opportunity, and motivation leading to behaviour, we now have behaviour impacting the three factors. By improving their skills, they are improving their capability. By playing and improving, they get more game time on the pitch/court/field as they are selected for their school team to play against other schools; behaviour thus enhances opportunity. The enjoyment being a source of active engagement with their sports club; they thus want to play more often, and behaviour increases motivation.

Capability and opportunity can have both direct and indirect effects on behaviour because they can influence motivation as well as behaviour (Michie et al., 2011; Howlett et al., 2019). The bidirectional relationships and the indirect impact of capability and opportunity are shown below in a simpler version of the COM-B model

(see Figure 3.1). The more up-to-date and comprehensive version of the framework is shown in Figure 3.2. Aside from illustrating the subfactors, this version has two significant differences. Firstly, the relationship between capability and motivation is bidirectional. Secondly, motivation and opportunity no longer have a direct relationship with behaviour but now influence the relationship between motivation and behaviour (West and Michie, 2020). Although more complicated, behaviour is still fundamentally influenced by the three preceding factors of capability, opportunity, and motivation.



Figure 3.1: The “simple” COM-B model

Source: Barker et al. (2016)

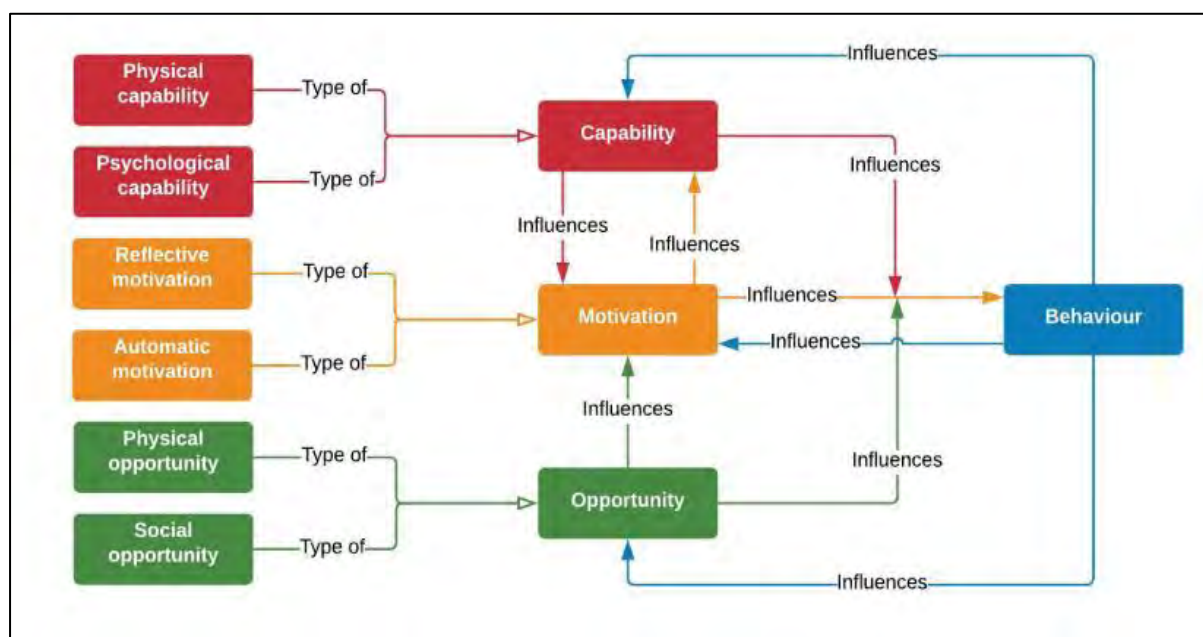


Figure 3.2: The “comprehensive” COM-B model of behaviour change

Source: West and Michie (2020)

The COM-B model can help banks to encourage their clients to behave more securely. However, this study focused on how the three COM-B factors come into play, considering the behaviours of those attempting to subvert account security. As mentioned in the first chapter, one of the goals of this study was to explore how people may rationalise decisions to commit fraudulent or dishonest actions.

To dissuade people from engaging in online banking fraud (change behaviour), nudging is employed to target these three subfactors. Thus the COM-B model serves as the theoretical framework for the study, as it deals specifically with how an individual's behaviour can be altered. In simpler terms, the nudges investigated in this study aim to make it more difficult for individuals to rationalise fraudulent behaviours in this context. The third goal exists to help clarify what rationalisations individuals may use when deciding to commit online banking fraud.

3.3 Dual Process Model

The dual process model used in psychology can be linked to the automatic and reflective motivation subfactors. This framework suggests that human decision making is an interplay between two systems. System 1 is intuitive, subconscious, faster, and inflexible, while System 2 is deductive, self-aware, slower, and more flexible (Hansen, 2016; Mirsch, Lehrer and Jung, 2017; Renaud et al., 2017; Speer, Smidts and Boksem, 2020). Overall this model is integrated into the COM-B model to some degree through the automatic and reflective motivation subfactors. System 1 leans heavily towards value-driven or automatic motivation, while System 2 leans more towards reflective motivation. People prefer to use System 1 because it allows for quick and efficient decision-making via heuristics or “rules of thumb”, despite the risk of developing biases (Mongin and Cozic, 2014). Nudges can be used to target either of these decision-making systems to alter individuals’ behaviour; i.e., they can be used to combat or exploit human heuristics and biases to lead to better decision-making (Acquisti, 2009; Caraban et al., 2019). Table B1 and Table B2 in Appendix B provide clarity on what (sub)factors the nudges employed were targeting.

3.4 The Traditional Economic Model

Before considering rationalisations, it is worth mentioning one key observation. Individuals often do not behave like the perfectly rational human being described in economic theory (Ariely, 2012; Gerlach, Teodorescu and Hertwig, 2019). This hypothetical perfectly rational human being is often referred to as “*Homo economicus*” (Bazerman and Gino, 2012). *Homo economicus* always uses all the objective information they have available to make informed decisions based on a relatively simple cost-benefit analysis of how much “utility” (satisfaction or benefit) they will receive from their potential options (Mazar, Amir and Ariely, 2008; Shalvi et al., 2015). *Homo economicus* remains consistent in their decision making, and is unaffected by emotions or circumstances. They seek, above all else, to maximise utility; thus, if one option objectively gives them more utility, according to economic theory, *Homo economicus* will always choose it. As a result, information regarding morality and ethics, which often tend to be subjective, is generally excluded from the decision-making process. As a result, the “perfectly” rational decision they make can be completely immoral or unethical. It is also worth noting that System 1 thinking often tends to encompass heuristics, habits, and bias, which often lead to human beings making less-than-perfect decisions (Broers et al., 2017). These heuristics are used as coping mechanisms or shortcuts to help make quick decisions when inundated with excess information. Overall this model, whilst limited and not applied too much in this study, is highlighted as the literature makes it clear human behaviour is not always perfect (utility maximising), and what we observe people may seem irrational or less than ideal. This touches on the rationalisations aspect, as people deviate from the perfect *Homo economicus* for a variety of reasons that this model may struggle to incorporate.

3.5 Rationalisation and Dishonesty

Within the literature reviewed for this study, the rationalisations that individuals may use for engaging in fraudulent behaviour often followed one of two paths. Although different, these paths share a key similarity in that they deal with the individual’s perception of how moral or good they are. The first path, known as the theory of self-concept maintenance, has an internal focus and deals with self-image and morality

(Mazar et al., 2008; Gneezy, Kajackaite and Sobel, 2018). The second path, known as the guilt aversion hypothesis, takes a more external perspective and looks at social norms and guilt (Chang et al., 2011; Khalmetski, 2016; Cartwright, 2019). The former looks at whether the individual still sees themselves as a good person, while the latter deals with whether the individual believes others would still consider them a good person. In terms of the literature, most did not use the term or focus on “fraudulent” behaviour specifically but broadened the scope to include literature related to dishonest behaviour.

Ariely (2012), in his book on dishonesty, used the term “fudge factor” to describe a phenomenon that is also relatively common in other literature. Mazar et al. (2008) and Gneezy et al. (2018) also refer to the same phenomenon and call it the theory of self-concept maintenance. Generally speaking, the phenomenon explains how individuals only partially cheat (forgo the maximum potential benefit) so as to retain a positive self-image of being a good person while behaving dishonestly (Mazar et al., 2008; Bazerman and Gino, 2012; Gravert, 2013; Schuchter and Levi, 2013; Rosenbaum, Billinger and Stieglitz, 2014; Shalvi et al., 2015; Gächter and Schulz, 2016; Syofyan, Pradini and Kurniawati, 2017; Cohn et al., 2019; Holt, 2019; Speer et al., 2020). In simpler terms, individuals convince themselves (rationalise) that they are a good person because they did not take full advantage of an opportunity while still reaping benefits from dishonesty. Using the example of online banking fraud, after logging in to someone else’s account using compromised credentials, the third party sees a balance of R20 000. Rather than steal the full R20 000, they “only” transfer R200 into their own banking account. After this, they leave the rest of the funds untouched and log out of the compromised account. The third party, in this case, has rationalised their behaviour by convincing themselves they are still a good person, even after committing fraud because they only stole “a little” rather than everything in a compromised account. They rationalise that the affected account holder can afford to lose what they stole, and since they had a bill to pay, they had no choice.

The core idea of this path is that individuals will go to surprising lengths to protect their positive self-image. Shalvi et al. (2015) found that these justifications can be used before or after dishonest behaviour, as long as moral self-concept can be maintained. Individuals experience some form of guilt or distress when they behave in a way that is inconsistent with their self-image because it means that their self-image will need to

be updated, and they thus seek to avoid this (Aquino et al., 2009). In other words, they do not want to see themselves as cheaters, fraudsters, or thieves. The third party in the previous example would therefore not see themselves as a thief for stealing the R200 because they left significantly more in the account than they stole. An interesting aspect of the fudge factor is that it can apply even when the individual is aware that there is little to no chance of being caught and facing the consequences of their dishonest behaviour (Ariely, 2012; Rosenbaum et al., 2014). If we alter the previous example, the third party in question would still not steal the full R20 000, even if, hypothetically, they could convert the funds into cryptocurrencies that they were sure the banks would not be able to trace back to them.

The fudge factor, while useful, does have limitations regarding explaining the behaviour of individuals who are facing temptations. Even in the experiments where it was observed, it did not explain all behaviours; some people still cheated completely to reap the full potential rewards (Gravert, 2013; Gneezy et al., 2018). One possible explanation for those who cheated completely within these honesty experiments and studies was that they believed detection was improbable (Batson, Thompson and Chen, 2002; Gravert, 2013; Gneezy et al., 2018). Going back to the previous example, the third party may have stolen only R200 because they believed the smaller fraud was more likely to “slip under the radar” (go unnoticed). The fudge factor is also interesting because it contradicts traditional economic theory (Gerlach et al., 2019). Suppose the third party behaved like *Homo economicus*, then they should have taken all the money in the account, irrespective of the rather non-trivial chances of being caught. They could use the R20 000 to buy more goods and services to give themselves more utility. Those individuals in the honesty experiments who took all the money behaved more in line with traditional economic theory. Overall, the fudge factor, while not perfect, emphasises the importance of a moral self-image and how it may impact behaviour and rationalisations. Where the fudge factor had a more internal perspective with the focus on self-concept, the second path shifts to a more external focus.

The guilt aversion hypothesis tends to encapsulate the broader theme of this path. The guilt aversion hypothesis states that people experience stress or guilt when they behave in ways that are inconsistent with what they believe others expect from them (Battigall and Dufwenberg, 2007; Chang et al., 2011; Kawagoe and Narita, 2014;

Khalmetski, 2016; Molnár and Chaudhry, 2018; Speer et al., 2020). This can be easily applied to values such as trust, honesty, and self-control, which are often internalised social norms (Mazar et al., 2008; Rosenbaum et al., 2014; Mooijman et al., 2018). In essence, this path looks at scenarios where individuals try to avoid behaving in ways they believe their peers or society would frown on. This guilt limits or, in some cases, prevents dishonest behaviour carried out by the participant, even in cases where the individual can cheat or be dishonest without being caught (Mehlkop and Graeff, 2010; Abeler, Nosenzo and Raymond, 2019). Thus, similar to the fudge factor, an individual may forgo potential monetary gains of dishonest behaviour. Going back to the example, this would refer to a third party who decides to alert the bank or the account holder about the compromised account because their parents, their schools, and the media they have consumed have “hammered home” the message that it is wrong to steal.

The literature suggests that social norms can exert an impact on behaviour, but as much as they may encourage honest behaviour and actions, they can also potentially encourage dishonest or immoral behaviours (Mehlkop and Graeff, 2010; Ariely, 2012; Schuchter and Levi, 2013; Gächter and Schulz, 2016; Syofyan et al., 2017). If the social culture around an individual does not frown on theft or even actively encourages it, it can make it very easy for an individual to commit fraud (Syofyan et al., 2017). When stealing, the individual would likely feel less need to justify their behaviour because it is socially acceptable. Beyond the subfactors related to rationalisations, this also tends to lean into the social opportunity subfactor of the COM-B model. Going back to the example, suppose the third party in question worked for an organisation that had a culture that encouraged bribery and corruption. When the third party stumbles upon someone else’s bank credentials, they are far more likely to take the full R20 000 in the account without batting an eye. While not necessarily a limit of the guilt aversion hypothesis, this does show a hypothetical scenario in which the phenomenon might also push people towards dishonest behaviour.

Social norms also tie into another important aspect of the guilt aversion hypothesis, namely the impact of second-order beliefs on behaviour. Second order refers to the fact that the moral standards or expectations people try to compare themselves to may not be perfectly accurate; it is what the individual believes is expected of them by others (Mehlkop and Graeff, 2010; Khalmetski, 2016; Molnár and Chaudhry, 2018;

Cartwright, 2019). As a result, the guilt aversion hypothesis has a more external focus than the fudge factor. The social norms, which initially are external to the individual, are internalised to create expectations and standards that an individual uses to hold themselves accountable to; they can thus also affect self-concept (Mehlkop and Graeff, 2010; Kuhfuss et al., 2016). In one way or another, guilt aversion and the fudge factor deal with individual perception of being an honest individual; the former to others (external) and the latter to themselves (self-perception). People will use rationalisations to ensure they maintain a positive moral perception of who they are. These rationalisations focus more on reflective motivation because individuals think of ways to justify their dishonest actions consciously (Speer et al., 2020).

Overall, these rationalisations help explain why an individual's behaviour may deviate from the utility maximising goal of the traditional economic model, as it does not incorporate the relatively subjective aspect of moral perception in controlling behaviour despite its importance. These rationalisations are discussed in subsequent chapters (see Chapter 6.5 and Chapter 7.5) to explain what the study found and how closely it aligned with this theory.

3.6 (Dis)honest Behaviour

The previous subsection focused on how people may rationalise dishonest behaviour by looking at the guilt aversion hypothesis and the fudge factor. This section examines the findings of other research regarding dishonest behaviour.

Fraud can be considered as one way that individuals can be dishonest as it is a form of theft (Lewicki and Stark, 1996; Scott and Jehn, 2003). In the model by Lewicki and Stark (1996), dishonesty is envisioned as a three-dimensional construct (see Figure 3.3). At the centre of the construct is honesty, which branches into three paths, each covering a different principle related to honesty. The principles are respect for property, rule-following, and truthfulness. When one or more of these principles are violated, it results in some form of dishonesty. These violations are theft, rule-breaking, and lying. The model is illustrated below.

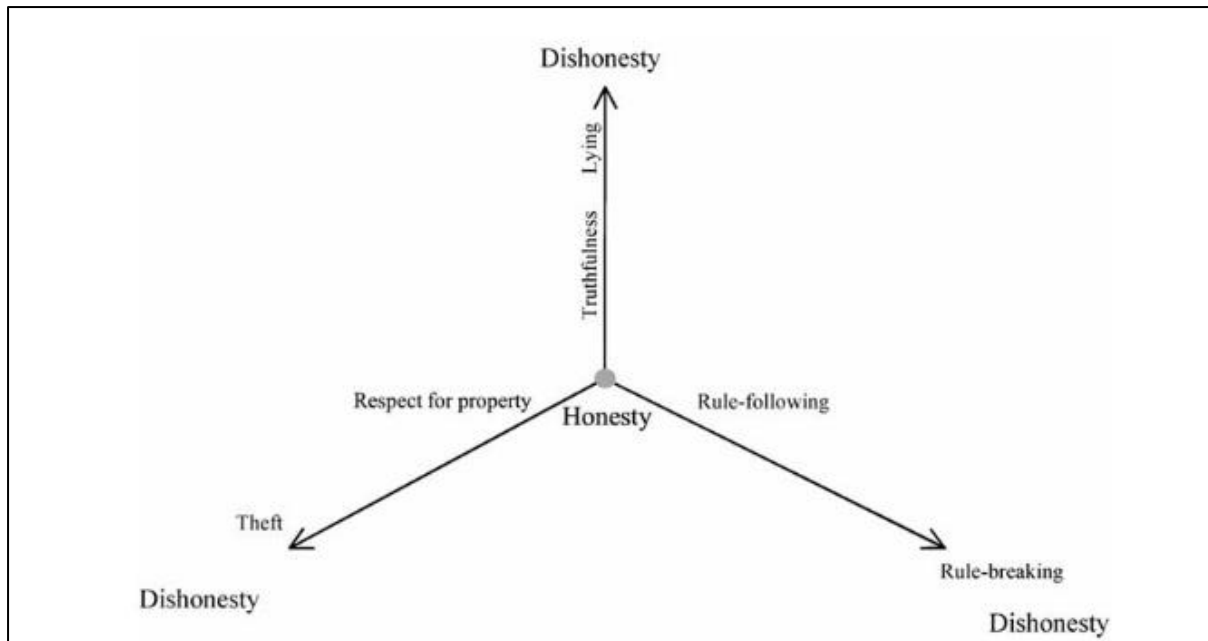


Figure 3.3: Dishonesty conceptualised as a three-dimensional construct

Source: Scott and Jehn (2003)

Köbis et al. (2019) raise the question of whether or not people are intuitively dishonest or honest. In their meta-analysis of honesty-related literature, they did find some evidence for both sides of the debate. This question is also encapsulated by the “Will and Grace hypothesis”, which encapsulates the idea that along a spectrum, there are two polar opposites concerning moral behaviour (Speer et al., 2020). At one end, the “Will hypothesis” explains that people are naturally dishonest and selfish and need to put in some form of mental effort to behave honestly. At the other end of the spectrum, the “Grace hypothesis” proposes that people are naturally honest and altruistic and need to engage in some form of mental effort to justify dishonest or selfish behaviour. In simpler terms, the question of institutive (dis)honesty deals with the individual’s behaviour when they mostly rely on System 1 thinking. With the Will hypothesis, behaviour tends to deal more with self-control issues, while the Grace hypothesis tends to lean more towards issues like succumbing to temptation (Amigud and Lancaster, 2019; Speer et al., 2020). Most people are somewhere between the two extremes of the Will and Grace hypothesis and encounter a hybrid of the issues suggested, depending on the circumstances. Overall, the mental effort exerted to overcome an individual’s “default” illustrates how System 2 thinking, thus reflective motivation, often comes into play in decisions regarding honesty (Aquino et al., 2009; Speer et al., 2020).

Exerting some form of effort beforehand is often used to justify behaving dishonestly (Gravert, 2013; Amigud and Lancaster, 2019). Individuals rationalise that having already invested some form of effort, they can “take a shortcut” towards achieving the final goal. According to Gravert (2013), dishonesty (cheating) also tends to be easier to justify when the outcome is based on chance. People also tend to find it harder to be honest when they have completed (mentally) taxing tasks or, in general, are just tired (Ariely, 2012; Amigud and Lancaster, 2019). This suggests that when System 2 thinking is overtaxed, people can fall back upon System 1 thinking; thus supporting the Will hypothesis.

Situational cues can influence behaviour (Bazerman and Gino, 2012). According to Aquino et al. (2009), this can occur due to these situational cues making moral identity within moral self-concept more or less accessible. In the case of the former, situational cues could encourage more honest behaviour, while in the latter, they could encourage more dishonest behaviour. Ariely (2012) mentions that in previous experiments, he found something similar by using a moral prime in the form of reading the Ten Commandments or an honour code. In the experiment, he could significantly decrease the cheating (dishonesty) rate. This was mediated by the centrality of moral identity within an individual’s self-concept or, in other words, how important behaving morally and honestly was to the individual (Aquino et al., 2009). Information regarding the dishonesty of others is another situational factor (Gerlach et al., 2019). This ties in with the influences of social norms mentioned earlier with the guilt aversion hypothesis. Learning that other people have also behaved dishonestly makes it easier for an individual to behave in a similar manner (Ariely, 2012).

One situational cue worth mentioning is financial incentives; this is one of the factors that may encourage more dishonest behaviour. The size of the financial incentive can impact people’s decision to behave (un)ethically (Gneezy et al., 2018; Gerlach et al., 2019). Khalmetski (2016) and Mazar et al. (2008) suggest a hypothetical threshold of increasing financial incentives beyond which people will behave dishonestly and decide to steal. However, this refers more to a binary decision regarding whether or not to steal. Applying it back to the compromised credentials example, it is easier to steal from an account with a balance of R20 000 than an account with a balance of R200. The latter case of R20 000 is more likely to have passed the threshold, while in the former, a third party is more likely to decide to leave the funds completely

untouched. Beyond the binary decision to steal or not steal, there is the question of how much to steal. Gneezy et al. (2018) found that it is easier to justify stealing relatively small amounts of money. This is in line with the fudge factor, as stealing a “little” is relatively easy to justify. It can also line up with the findings of Khalmetski (2016) because the small amount is relative. Using the previous example, if the third party decided to take R100, proportionally, it has far less of an impact on the account with R20 000 than the one with R200. Their fraudulent behaviour is thus easier to justify in the latter case, where the victim is wealthier. It is worth noting that in his book, Ariely (2012) disagreed with the idea that the size of the financial incentive impacted dishonesty.

Still linked to the influence of financial incentives, a conflict of interest can also cause an individual to behave more dishonestly (Ariely, 2012; Bazerman and Gino, 2012; Segal, 2020). The broader theme of the conflict between self-interest and altruistic or honesty-related motivations is relatively common (Lewicki and Stark, 1996; Batson et al., 2002; Fehr and List, 2004; Aquino et al., 2009; Piquero et al., 2011; Ariely, 2012; Bazerman and Gino, 2012; Cohn et al., 2019; Köbis et al., 2019; Speer et al., 2020).

Moving beyond situational cues, the last factors this study considers are who benefits, who is hurt, and monitoring. Individuals can be dissuaded from dishonesty when there will be a concrete victim (Ariely, 2012; Köbis et al., 2019). In other words, it was harder to be dishonest when the person who would suffer due to their behaviour was someone they could either identify or empathise with. Using the compromised user credentials example, if the third party discovered that the account holder is one of their classmates they encounter and talk to daily, chances are they would find it harder to steal from their account. Ariely (2012) found that cheating (dishonesty) is more common when the perpetrator knows that others will benefit from their dishonesty. Returning to the compromised credentials example, the third party would find it much easier to defraud the account holder when he/she believes the money will help his/her family. Increasing monitoring tends to encourage honest behaviour (Rosenbaum et al., 2014). This finding is unsurprising as more monitoring implies increased chances of dishonesty being detected, and thus the individual facing undesirable consequences for their actions.

This section focused on literature regarding dishonesty. The overall results of the literature search regarding honesty are presented in Table 3.1. The first column is related to all the influences or factors that can affect an individual's behaviour according to the literature. In the two columns, "Dishonesty" and "Honesty", Y represents some form of correlation or association. With the exception of 'Conflict of Interest' and 'more random or chance-based outcome', these factors are alluded to in Chapter 6 and Chapter 7 to some degree (i.e. they arose after analysing the interview transcripts and the discussion of the study's overall findings).

Table 3.1: A summary of the findings regarding honesty

| Influence/Factor | Dishonesty | Honesty | COM-B factor |
|--|------------|---------|-------------------------|
| (Mental) exhaustion | Y | | Capability, motivation |
| Social norms | Y | Y | Motivation, opportunity |
| Financial incentives: Size | Y | | Motivation |
| Conflict of interest | Y | | Motivation |
| Monitoring | | Y | Motivation, opportunity |
| Empathy/sympathy with potential victim (concrete victim) | | Y | Motivation |
| Effort exerted has already allowed partial completion of goal(s) | Y | | Capability, motivation |
| More random or chance-based outcome | Y | | Capability, motivation |
| Moral reminder / prime | | Y | Motivation |

3.7 Summary

This chapter examined the behaviour and rationalisations of individuals in various scenarios where their honesty/integrity may be tested. The main theoretical framework of the study, the COM-B model of behaviour change, was introduced. The dual process and the traditional economic decision-making models were also briefly discussed. The subsequent chapter is the final chapter of the literature review, which examines nudging.

CHAPTER 4:

NUDGING

4.1 Introduction

This chapter focuses on the exploration of nudging-related literature. The goal of this chapter was to explain nudging in more detail. A brief look was taken at other behavioural interventions before going into a short summary explanation of the various nudging techniques found within the literature. (For more information about how papers were selected for inclusion in the literature review, see Chapter 5.5.1)

4.2 Nudging

Nudging is a behavioural intervention based on the work of Thaler and Sunstein (2008). A nudge is a choice architecture manipulation designed to alter people's behaviour predictably, without restricting any options, and without significantly changing a person's economic incentives (Thaler and Sunstein, 2008; Lembcke et al., 2020). Choice architecture generally refers to the context in which a decision is made, while the choice architect refers to the individual or organisation that designs or alters the choice architecture (Thaler and Sunstein, 2008). The choice architect uses a nudge to guide the nudgee or targeted individual(s) towards a better decision (Renaud and Zimmermann, 2018). What is considered "better" can be debatable, but this will be discussed along with the concepts of pro-social vs pro-self-nudges.

Nudges, in general, are closely linked to the concept of "libertarian paternalism" (Thaler and Sunstein, 2008; Calo, 2014; Hansen, 2016). Libertarian paternalism refers to intervening in or manipulating the behaviour or decisions of other individuals as long as these interventions preserve individuals' freedom to choose different options or alternatives (Mirsch et al., 2017). Unlike other forms of paternalism, it considers individual preferences. The manipulations are designed to guide individuals to make decisions or behave in ways that improve their welfare (Barton and Grüne-Yanoff, 2015). The rest of this section considers different aspects of nudging and interesting findings.

Previous research has already applied nudging in a range of contexts. Digital nudging refers to the application of nudging through the design of the user interface (UI) and interaction elements within a website or software application (Mirsch et al., 2017; Franco, 2018; Lembcke et al., 2020; Jesse and Jannach, 2021). Thus, in the case of online banking and, more broadly, digital nudging, the choice architecture refers to the design of the interactions and interface of the banking website. The choice architects would be the bank and its website developers. One important principle worth mentioning regarding nudging is that “there is no neutral design” (Thaler and Sunstein, 2008; Broers et al., 2017). This means that no matter how the choice architect designs a website, there is always some subtle “push” towards certain options. Using an example from the context of the study, a bank offers new clients the opportunity to open up a new bank account on its website. When potential clients visit the website after entering their details, they can choose which type of account they wish to open. By default, the first option to open a new account would be a current account. Potential clients can still choose money market accounts, retirement accounts, or savings accounts (Hargrave, 2021). By simply being the first or default option, people who simply want a bank account more often than not create current accounts. Even though the bank offers several accounts by arranging them alphabetically, they still give some new clients a subtle “push” towards opening current accounts by listing them first. Default options are one of the potential nudging mechanisms noted in the article by Jesse and Jannach’s (2021) article.

Earlier in this section, the idea is that the nudges are meant to alter the behaviour of a nudgee in such a way that they make a better decision. Thus arises the potential question: The decision that is better for whom? The concepts of pro-social and pro-self nudges are very helpful when it comes to answering this question (Hagman et al., 2015). Pro-social nudges refer to nudges that attempt to guide nudgees towards choosing options that are better for society as a whole (Barton and Grüne-Yanoff, 2015; Hagman et al., 2015; Renaud and Zimmermann, 2018). An example of this would be a nudge that aims to get more people to recycle. This nudge could help reduce environmental waste, but it does not significantly benefit the nudgee. Pro-social nudges have also been referred to as social nudges (Nagatsu, 2015). On the other hand, pro-self nudges are meant to guide nudgees towards decisions that improve the welfare of the nudgee (Barton and Grüne-Yanoff, 2015; Hagman et al., 2015; Renaud

and Zimmermann, 2018). An example of a pro-self nudge would be trying to encourage someone to exercise more often; this could lead to a healthier lifestyle for the nudgee. There can potentially be a slight overlap between the pro-social and pro-self, but, generally, social nudges have a broader scope in terms of their goals. Overall, nudges are meant to provide some form of positive (social) benefit for the nudgee or society at large. Encapsulating this idea is the slogan “Nudge for good” that Thaler includes when he signs copies of his and Sunstein’s book (Hansen, 2016).

Despite nudges being meant to encourage beneficial behaviour, individuals and organisations have found ways to use the intervention to manipulate people into choosing undesirable options. Such nudges tend to lead the nudgee to the decision that leaves them worse off (Hollingworth and Barker, 2017; Renaud and Zimmermann, 2018; Sunstein, 2019). The official term for such nudges is “sludge” or “dark patterns” (Sunstein, 2019; Luguri and Strahilevitz, 2021). In the context of websites and e-commerce, we can use the example of companies using digital nudges to get people to buy more expensive goods or services than they need (Ivanova, 2021; Luguri and Strahilevitz, 2021). The nudgee would have wasted their hard-earned money, but the company would have a better bottom line. “Nudge for good” implies that such abuses or manipulations are not nudges.

Nudges are meant to be cheap, and their direction possible to avoid (Thaler and Sunstein, 2008; Broers et al., 2017). This ties into one aspect of the definition of nudges, “without restricting” any options. The nudgee is free to ignore the nudge and choose any other options available; the nudge is therefore optional. This is a key link between nudging and libertarian paternalism, specifically the libertarian part, which refers to “liberty-preserving” policies (Sunstein, 2014). Looking back at nudge for good, we can also see the paternalism aspect. The paternalism link refers to organisational or governmental policies designed to guide people towards better decisions (Thaler and Sunstein, 2008; Hansen, 2016). Nudges are often linked to libertarian paternalism but are not synonymous and interchangeable (Hansen, 2016). Thaler and Sunstein (2008) clarify that nudges can only count as libertarian paternalistic when the difference in option costs, both cognitive and incentive wise, is low.

Looking at the paternalism aspect of nudging and Section 2.3, humans do not always make the best decision in part due to heuristics and biases (Kahneman, 2003). Unlike

other interventions that try to eliminate or circumvent these biases, nudges often (target and) exploit heuristics and biases in human decision making (Mongin and Cozic, 2014; Renaud and Zimmermann, 2018). As a result, nudges can often be ignored by *Homo economicus* (Mongin and Cozic, 2014; Hansen, 2016). Nudges can also combat irrationality by encouraging more reflective thinking (Hansen, 2016; Renaud and Zimmermann, 2018). As a result, nudges can target System 1 and System 2 thinking, and thus affect automatic and reflective motivation.

Overall, nudges are well suited to altering automatic motivation, but they can still affect reflective motivation and encourage more profound thought and consideration. From the literature, it is not immediately apparent how nudges would directly impact psychological capability. Suggesting the influence of nudging on psychological capability would be more indirect. Although given the definition of psychological capability in Section 3.2, any nudge that does help improve the nudgee's skills, knowledge, or understanding of their options can qualify. This broad classification, in combination with digital nudging's focusing on interactions and UI, i.e. what the user can see and how they interact with the site, most nudges can be mapped onto the COM-B factor. This can be seen in how most of the nudge mechanisms mapped in Table 4.2 are under capability. Digital nudging has been employed in previous research and literature and served as a guide for this study.

Calo (2014) and Renaud and Zimmermann (2018) describe nudging and three other behavioural interventions. The first intervention, known as a "code", describes a change to the environment, which makes the undesirable behaviour or choice significantly more difficult for an individual. Calo (2014) uses a speed bump as an example: drivers need to slow down to go over the hump comfortably, but they can still speed over it even though this would be uncomfortable for the passengers. The second intervention Calo (2014) describes is called a "notice", which refers to the simple provision of extra information. Ideally, this would prompt additional reflection by an individual and cause them to change their behaviour, but they are ineffective alone (Calo, 2014).

The final behavioural intervention they describe is called "prods". Through the use of irresistible manipulations, these interventions are more controlling than nudges (Calo, 2014). In terms of nudging, Calo (2014) splits them into simple nudges and hybrid

nudges. The simple nudge is more in line with the definition and aspects of nudging looked at thus far (Calo, 2014; Hansen, 2016). For a quick recap, a nudge is deliberate choice architecture manipulation, designed to influence behaviour predictably by exploiting human biases and heuristics to get an individual to make a better decision without blocking any of the individual's options or significantly changing their (economic) incentives. The hybrid nudge is a combination of a simple nudge and any of the other behavioural interventions. Renaud and Zimmermann (2018) summarise all five behavioural interventions in Table 4.1. The following section examines all the nudging mechanisms found in the literature.

Table 4.1: The five behavioural interventions

| Type | Code | Simple nudges | Prod | Notice | Hybrid nudges |
|---|--|--|---|---|--|
| Influenced by: | Manipulating the choice architecture to make the undesirable option or behaviour very difficult. | A nudge that aims to trigger or exploit shallow cognitive process, i.e., System 1, or heuristics and bias. | Triggers shallow cognitive processes that are very difficult to resist. | Provides additional information (only) to prompt an individual to think or reflect. | Combination of a simple nudge and additional behavioural interventions targeting reflective reasoning. |
| Targets | N/A | Human bias or System 1 | Human bias or System 1 | Reflective or System 2 | Both Systems 1 and 2 |
| Individual's awareness of intervention | Unaware | Unaware | Unaware | Aware | Aware |
| Length of effect | Short | Short | Short | Short and long term | Short and long term |
| Examples | Speed bumps and speed limits | Defaults | Irresistible limited-time-only offers | Product warnings | Contrasting current speed to the speed limit of the road |
| Information security and privacy | Blocking USB ports | Colour coding Wi-Fi networks (Jeske et al., 2014) | Privacy-invasive defaults (Obar and Oeldorf-Hirsch, 2020) | Privacy policies (Obar and Oeldorf-Hirsch, 2020) | Prompting stronger passwords (Renaud and Zimmermann, 2019) |

Source: Reproduced from Renaud and Zimmermann (2018:39)

4.3 Nudging Techniques and Interventions

In their original book, Thaler and Sunstein (2008) define six principles of good choice architecture; they created the mnemonic N.U.D.G.E.S. to help readers remember these principles. The six principles are “**i**Ncentives. **U**nderstand mappings. **D**efaults.

Give feedback. **E**xpect error. **S**tructure complex choices”. Since the book’s release, other researchers have gone beyond these six principles and devised or identified various nudging mechanisms. Ioannou et al. (2021) conducted a systematic literature review regarding nudging and privacy disclosures. They categorised the interventions they found into five categories: presentation, information, combination, defaults, and incentives. Mirsch et al. (2017) explored existing literature and noted the several psychological effects that nudging and libertarian paternalism could exploit. From the most to the least common psychological effects they found were framing, status quo bias, social norms, loss aversion, anchoring and adjustment, hyperbolic discounting, decoupling, priming, availability heuristic, commitment, mental accounting, optimism and overconfidence, attentional collapse, messenger effect, image motivation, intertemporal choice, representativeness, endowment effect, and the spotlight effect. Caraban et al. (2019) found 23 nudging mechanisms and grouped them into six categories: facilitate, confront, deceive, social influence, fear, and reinforce. Jesse and Jannach (2021) identified 87 nudging mechanisms through their systematic literature review. They were categorised into four broad categories and 13 smaller subcategories. Jesse and Jannach’s (2021) taxonomy of nudging mechanisms builds on another taxonomy created by Münscher, Vetter and Scheuerle (2016) by adding a fourth category. Overall, the taxonomy by Jesse and Jannach (2021) and the nudging mechanisms encompassed the six principles of good choice architecture and the nudging mechanisms from the other literature. It provides a useful summary of potential mechanisms that could be employed. Included in the nudging mechanisms are some of the psychological mechanisms mentioned by Mirsch et al. (2017). Figure 4.1 illustrates the taxonomy of nudging mechanisms (Jesse and Jannach, 2021). The subsections after this figure briefly explain each category and subcategory of nudging mechanisms. An expanded version of these subsections explaining each of the nudging mechanisms can be found in Appendix A.

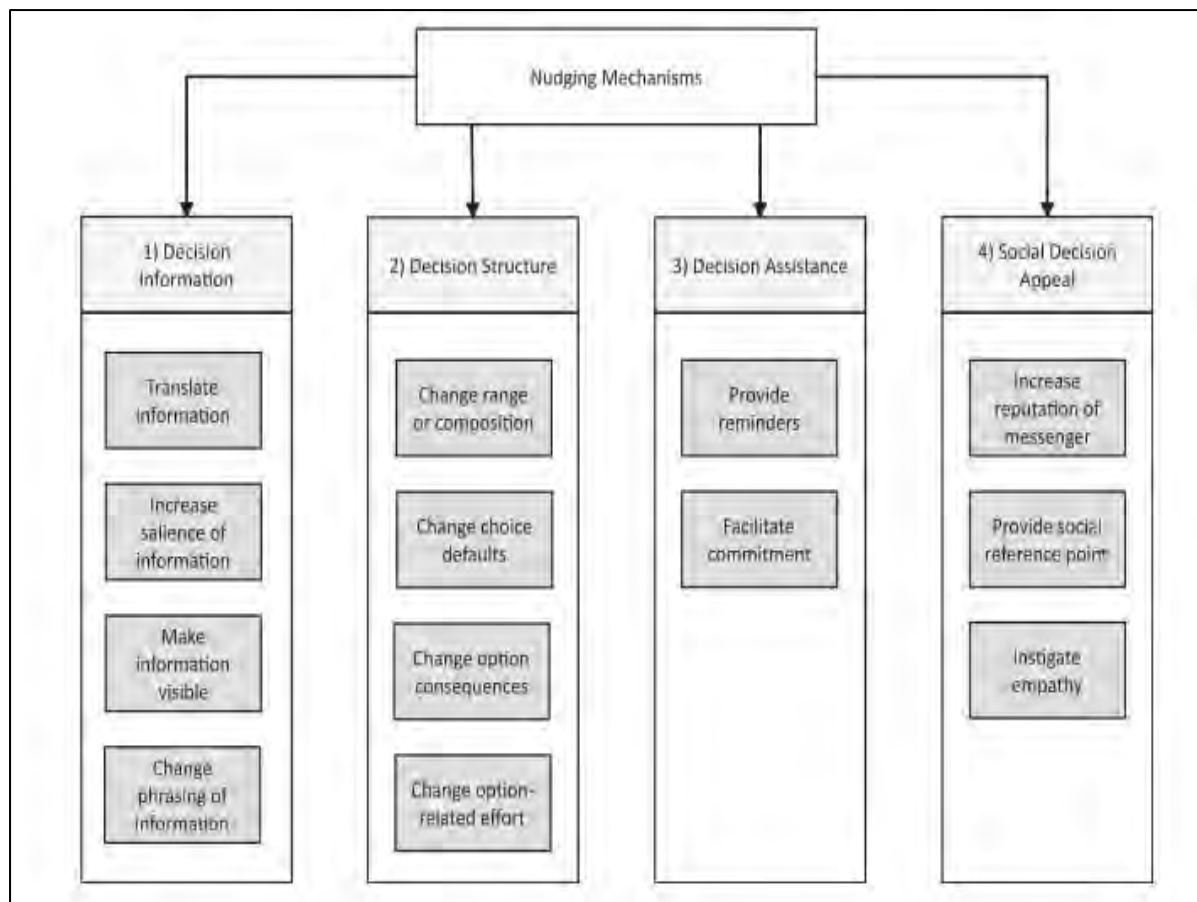


Figure 4.1: Taxonomy of nudging mechanisms

Source: Jesse and Jannach (2021)

The four main categories of nudging mechanisms are decision information, decision structure, decision assistance, and social decision appeal (Jesse and Jannach, 2021). Social decision appeal is the category added beyond the original taxonomy by Münscher et al. (2016). While other studies also examined similar nudging mechanisms, Jesse and Jannach (2021) provide the most comprehensive summary of the nudging mechanisms. It's worth mentioning that in Figure 4.2, Figure 4.3, Figure 4.4 and Figure 4.5, the bullet points in the extracts from Jesse and Jannach (2021) have been replaced to indicate if and where a nudge mechanism may have been employed. The normal black bullet represents nudges that were not employed, the red **X** represents nudge mechanisms employed on the PRE-LOG version, and the blue **#** represents the POST-LOG version. If and where nudges were deployed is also illustrated in the three rightmost columns of Table 4.2 in Section 4.3.4

4.3.1 Decision Information

Decision information refers to a category of nudges that impact what information is presented to the nudgee and how it is presented (Jesse and Jannach, 2021). The general goal with this category of nudges is to reduce the cognitive effort the user needs to understand what they are doing on the website. This category of nudges can be broken down into four subcategories: translate, salience, visibility, and phrasing. Figure 4.2 provides an overview of this category and all its nudging mechanisms. Decision information is also the category with the most nudging mechanisms among the four. By making it easier for the nudgee or user of the website to understand the information presented on the website, most information falls under the psychological capability factor of the COM-B model.

| 1) Decision Information | | | | | |
|--|---|--|---|---|---|
| Translate information | Increase salience of information | Make information visible | Phrasing of information | | |
| <ul style="list-style-type: none">• Decrease vagueness and ambiguity• Explicitly mapping• Simplification• Understanding mapping | <ul style="list-style-type: none">✗ # Attracting/Reducing attention• Hiding information✗ # Increase salience of attribute• Increase salience of incentives# Using visuals to deceive✗ # Using visuals to increase salience | <ul style="list-style-type: none">• Checklist• Customized information• Disclosure• Give comparative information✗ # Informing• Make external information visible | <ul style="list-style-type: none">• Providing an explanation• Providing feedback• Providing multiple viewpoints✗ # Reduce the distance• Suggesting alternatives• Visible goals• Warning | <ul style="list-style-type: none">• Anchoring and adjusting• Attentional collapse• Availability• Biasing the memory of experiences• Decoy effect• Endowment effect# Framing• Hyperbolic discounting• Image motivation | <ul style="list-style-type: none">• Limited time window# Loss aversion• Make resources scarce• Mental accounting# Optimism and overconfidence• Placebos• Priming✗ # Representativeness✗ Spotlight effect• Temptation |

Figure 4.2: Decision information nudges

Source: Jesse and Jannach (2021)

4.3.1.1 Translate Information

The translate information subcategory of nudges here focuses on summarising complex and/or large amounts of information into something easy to grasp. This helps

users understand the impact of their actions on the online banking account. All four of these nudges fall under the psychological capability factor of the COM-B model as they help the user to understand the information presented on the site better. As a result, it would allow them to use the website better.

4.3.1.2 Increase the Salience of Information

This subcategory of nudging mechanisms deals with making certain information or options more prominent on a UI to draw the user's attention. These options are more likely to stay at the forefront of the users' thoughts as they navigate the website (Jesse and Jannach, 2021). For the most part, this subcategory of nudges is linked to psychological capability as it makes useful information more visible to users; thus helping them use the site better. The exception is deceptive visualisations, as images positively affect motivation, according to Caraban et al. (2019).

4.3.1.3 Make Information Visible

This subcategory focuses on providing pertinent information to the user to help them navigate the website/UI and decide on which option to take.

Most of the nudges within this subcategory also fall under psychological capability due to their focus on information. Exceptions are checklists, multiple viewpoints, reduce distance, and visible goals. Most of these exceptions fall under the reflective motivation factor of the COM-B model, according to Caraban et al. (2019). The checklist and visible goals make it apparent to users what they have accomplished thus far and what remains could motivate users to complete the process. Multiple viewpoints fall under motivation because they allow users to slow down, consider other people's opinions, and create an unbiased view. Reducing the distance, i.e., making potential problems "hit closer to home", can motivate users to consider them carefully.

4.3.1.4 Phrasing of Information

This subcategory of nudges focuses on changing how information is presented to the user to influence their behaviour. The focus on information also makes this subcategory of nudging mechanisms mostly fall under the psychological capability factor of the COM-B model. According to Caraban et al. (2019), placebos, decoys,

priming, and scarcity are exceptions in this subcategory and would likely fall under the motivation factor. Priming, for the most part, would fall under the subfactor of automatic motivation, as the stimulus the user is exposed to can easily be missed. For the most part, placebos, decoys, and scarcity would fall under reflective motivation as the users consider their options or think about seizing a “limited” opportunity in the case of scarcity.

4.3.2 Decision Structure

Decision structure refers to a category of nudges that focuses on the arrangement of options available to the nudgee (Jesse and Jannach, 2021). This category of nudges can be broken down into four subcategories: defaults, option-related efforts, range/composition of options, and option consequences. Figure 4.3 summarises all the nudges in this category.

| 2) Decision Structure | | | |
|--|--|--|---|
| Change choice defaults | Change option-related effort | Change range or composition of options | Change option consequences |
| <ul style="list-style-type: none"> • Automatic enrollment • Enhancing or influencing active choosing # Prompted choice • Setting defaults • Simplifying active choosing | <ul style="list-style-type: none"> • Change ease and convenience • Change financial effort • Change physical effort • Create friction • Navigability of contexts • Reduce paperwork • Speed bumps • Throttle mindless activity | <ul style="list-style-type: none"> • Change scale • Decision staging x # Order effects • Partition of options or categories • Structure complex choice • Structure of evaluation | <ul style="list-style-type: none"> • Change social consequences # Connect decision to benefit or cost • Micro-Incentives |

Figure 4.3: Decision structure nudges

Source: Jesse and Jannach (2021)

4.3.2.1 Change Defaults

This subcategory focuses on using the default option as a subtle nudge towards the desired option by using it as the default choice. When people have difficulty deciding, they may often resort to the default choice. These nudges often exploit the status quo bias: the reluctance to change existing or familiar circumstances and trying something new (Thaler and Sunstein, 2008; Caraban et al., 2019). The default nudges generally fall under the capability factor of the COM-B model as they all aim to simplify deciding for the user, although being forced to make an active decision does mean that a few of these mechanisms can overlap with reflective motivation.

4.3.2.2 Change Option-Related Effort

This subcategory focuses on creating an imbalance of effort required between the various options. In other words, make the more desirable options easier to take, while the less desirable options are harder for the nudgee to choose. Most of the nudges within this category fall under the capability factor of the COM-B model. In the context of an online banking website, these nudges would most likely fall under psychological capability. Still, they could also fall under physical capability and physical opportunity subfactors under different contexts. For example, placing healthy snacks at eye level at a food stand and making less healthy alternatives harder to see and reach. According to Caraban et al. (2019), friction is an exception as it creates reminders about alternatives and thus could fall under reflective motivation and physical opportunity.

4.3.2.3 Change Range or Composition of Options

This subcategory, as the name implies, focuses on the options presented to the user and how they are arranged or displayed to them.

The nudges under this subcategory would primarily fall under capability. They could also touch upon motivation and opportunity to a lesser extent, although opportunity again would be more context dependent than the other factors. In the context of online banking, arranging these nudges would affect how the functionality and various options of the site are displayed to the user. This could make it easier for the user to understand how to use the site as everything is grouped/arranged in a more intuitive

way. They therefore mostly fall under psychological capability and, to a lesser extent, physical capability, as visibility and positioning on the page can make certain options easier or harder to see and click (choose).

4.3.2.4 Change Option Consequences

This subcategory of nudges focuses on altering the potential consequences of each of the choices available to the user (nudgee). The goal is to tweak the consequences of the available options in such a way that the better options seem more appealing to the nudgee. Most nudges under this subcategory would fall under the reflective motivation subfactor. The additional information about the potential benefits or costs for each potential action would likely make the user or nudgee consider their options more. Social consequences, however, would also overlap with the social opportunity subfactor.

4.3.3 Decision Assistance

Decision assistance refers to a category of information that provides decision support to the nudgee (Jesse and Jannach, 2021). This category of nudges can be broken down into two subcategories: reminders and commitment. Figure 4.4 provides an overview of the nudging mechanisms under this category.

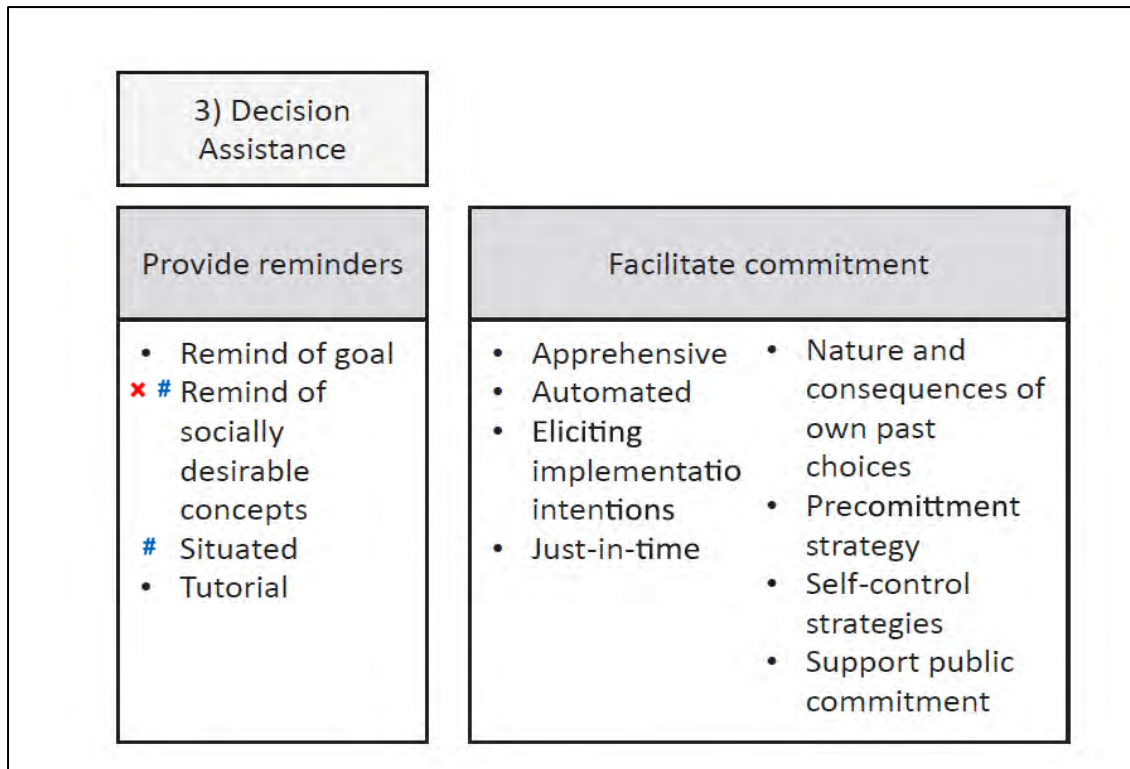


Figure 4.4: Decision assistance nudges

Source: Jesse and Jannach (2021)

4.3.3.1 Provide Reminders

This subcategory focuses on reminding users about their final goals and the potential benefit of completing a long process. The reminders themselves can also be used to promote the more desirable options. Among this subcategory of nudges, situated and tutorial would fall under the capability factor of the COM-B model. These nudges are meant to help provide some form of assistance to the user. The remaining two reminder nudges, “remind of goals” and “remind of socially desirable consequences”, fall under the reflective motivation factor, as they seek to get the individual to consciously reflect on certain goals and social norms.

4.3.3.2 Facilitate Commitment

These nudges focus on encouraging users to engage with their preferred option and stick with it until the end due to promises or pledges made to themselves or others. Most of the nudges in this subcategory would fall under reflective motivation as they focus on getting the user to slow down and consider their options, usually with some (long-term) goal in mind. Public commitment also falls under the reflective motivation

subfactor, but there is some overlap with the social opportunity subfactor by using social norms to influence behaviour. “Just-in-time”, being similar to tutorial and situated nudges, would also fall under the capability factor. In the context of online banking, this would mostly be psychological capability. Apprehensive and automated nudges also fall under capability. The former is because it gives the users various ways to use the website, and the latter is due to performing certain functions for the user and reducing the effort/input needed from them.

4.3.4 Social Decision Appeal

Social decision appeal is the final category of nudging mechanisms that focus on exploiting social influence and comparisons made by the nudgee (Jesse and Jannach, 2021). This category of nudges can be broken down into three subcategories: messenger reputation, social reference points, and instigating empathy. Figure 4.5 provides an overview of the nudges in this category.

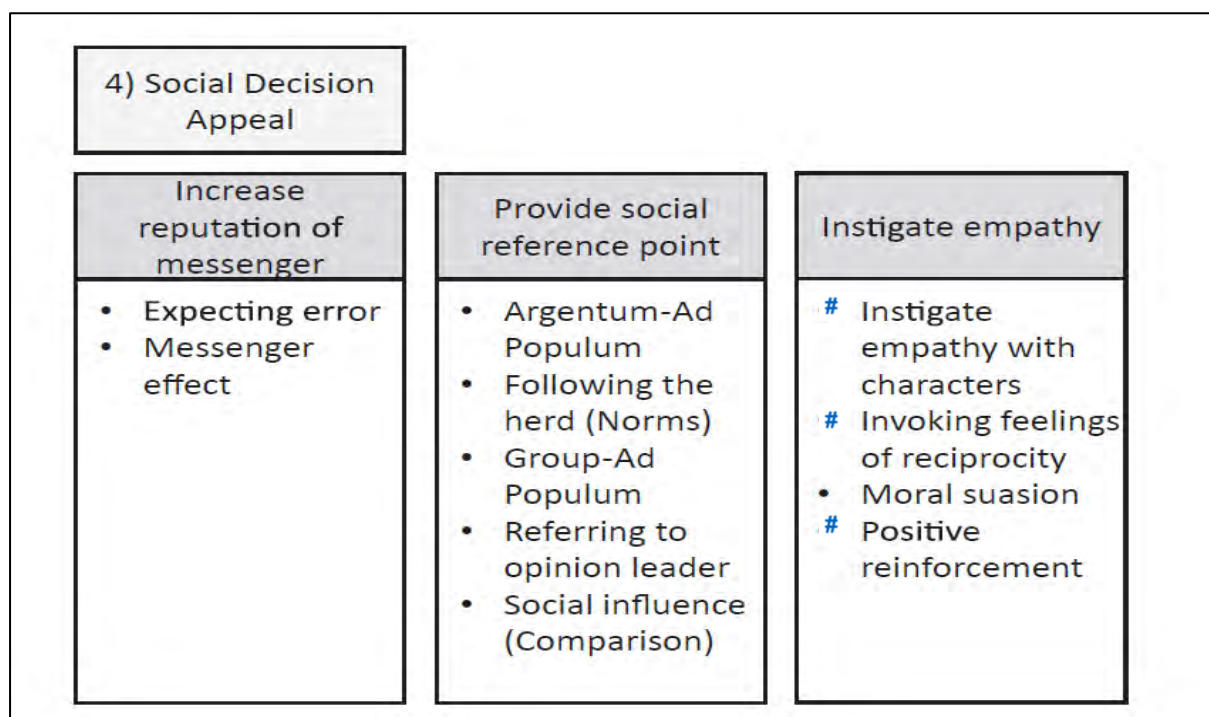


Figure 4.5: Social decision appeal nudges

Source: Jesse and Jannach (2021)

4.3.4.1 Increase Reputation of Messenger

This subcategory of nudges focuses on improving the reputation of the messenger – in this case, the bank and its website. The better the reputation of the messenger, the more the actual message they are trying to send will be taken to heart by the recipient – in this case, the user. Positive experiences can encourage clients to use their bank's online service more often.

As they are part of the broader social decision appeal, both these nudges naturally fall under the social opportunity subfactor. Expecting nudges, however, would also overlap with the capability factor.

4.3.4.2 Provide Social Reference Point

This subcategory of nudges focuses on exploiting social norms and comparisons to encourage certain behaviours or decisions. This entire subcategory of nudges would fall under the social opportunity subfactor. To some extent, they can also fall under the motivation factor; these nudges can sway users towards certain popular options or opinions of others.

4.3.4.3 Instigate Empathy

As implied by the name, this subcategory of nudges focuses on increasing the empathy the nudgee feels so as to encourage certain behaviours or choices (Caraban et al., 2019; Jesse and Jannach, 2021). By virtue of being part of the social decision appeal category, all the nudges under this subcategory should fall under social opportunity. Still, there is a significant overlap with other factors. Instigating empathy and positive reinforcement overlap with the capability factor as they can help the user learn and understand information from a digital interface. According to Caraban et al. (2019), reciprocation can also overlap with motivation.

The nudge mechanisms discovered, their explanations in Appendix A, along with Table B1 and Table B2 in Appendix B, helped clarify how the nudge mechanisms were expected to alter human behaviour (i.e. to which COM-B factors from Chapter 3.2 it could be mapped onto). The results are shown below in Table 4.2 (the table also points out which nudge mechanisms were employed). The main sources for the nudge

mechanisms and their mapping were the articles by Jesse and Jannach (2021), Caraban et al. (2019), and Münscher, Vetter and Scheuerle (2016). If the nudge mechanism, as understood from literature, affected skill, understanding, or the potential third party's ability to utilise the website's functionality, it was mapped onto capability and assigned a red dot. If the mechanism involved social influences that may permit or discourage certain behaviours or aspects of the physical environment described in the scenario (i.e. sticky note, isolation in an internet cafe) that could affect a third party's behaviour, it was mapped onto opportunity and assigned a green dot. Finally, if the mechanism touched on (targeted) the 'why' an individual may want to commit or avoid online banking fraud, consciously (reflective) or unconsciously (automatic), it was mapped onto the motivation factor and assigned an orange dot.

Although rare, some mechanisms could be mapped onto more than one COM-B factor and thus have multiple dots in Table 4.2. For example, with the 'increase salience of incentives' mechanism, by prominently placing the information and related link on its online banking page, a bank can make it clear that opening a new credit card may offer the client lower transaction costs and interest rates. Changing the positioning or prominence of the link also affects the client's capability, as it is easier to find access to this functionality (click). By informing them of the benefits of the credit card, it makes the client stop and consider whether or not to open a new card and thus can affect motivation.

Table 4.2: Nudges and COM-B factors - Main Sources Jesse and Jannach (2021), Caraban et al. (2019) and Münscher, Vetter and Scheuerle (2016)

| | Subcategory | Nudge | COM-B factor | | | Employed | PRE-LOG | POST-LOG |
|----------------------|--|---|-----------------|------------------|-----------------|----------|---------|----------|
| | | | ● Capability | ● Opportunity | ● Motivation | | | |
| Decision information | Translate the information | Decrease vagueness and ambiguity | ● | | | | | |
| | | Explicitly mapping | ● | | | | | |
| | | Simplification | ● | | | | | |
| | | Understanding mapping | ● | | | | | |
| | Increase the salience of the information | Attracting/reducing attention | ● | | | YES | ✓ | ✓ |
| | | Hiding information | ● | | | | | |
| | | Increase the salience of the attribute | ● | | | YES | ✓ | ✓ |
| | | Increase the salience of the incentives | ● | | ● | YES | | |
| | | Using visuals to deceive | | | ● | YES | | ✓ |
| | | Using visuals to increase salience | ● | | ● | YES | ✓ | ✓ |
| | Make the information visible | Checklist | | | ● | | | |
| | | Customised information | ● | | | | | |
| | | Disclosure | ● | | | | | |
| | | Give comparative information | ● | | | | | |
| | | Informing | ● | | | YES | ✓ | ✓ |
| | | Make external information visible | ● | | | | | |
| | | Providing an explanation | ● | | | | | |
| | | Providing feedback | ● | | | | | |
| | | Providing multiple viewpoints | | | ● | | | |

| | Subcategory | Nudge | COM-B factor | | | Employed | PRE-LOG | POST-LOG |
|---------|--------------------------------|-----------------------------------|-----------------|------------------|-----------------|----------|---------|----------|
| | | | ● Capability | ● Opportunity | ● Motivation | | | |
| □ ◊ ◊ ◊ | | Reduce the distance | | | ● | YES | ✓ | ✓ |
| | | Suggesting alternatives | ● | | | | | |
| | | Visible goals | | | ● | | | |
| | | Warning | ● | | | YES | ✓ | ✓ |
| | Change phrasing of information | Anchoring and adjustment | ● | | | | | |
| | | Attentional collapse | ● | | | | | |
| | | Availability | ● | | | | | |
| | | Biasing the memory of experiences | ● | | | | | |
| | | Decoy effect | | | ● | | | |
| | | Endowment effect | ● | | | | | |
| | | Framing | ● | | | YES | | ✓ |
| | | Hyperbolic discounting | ● | | | | | |
| | | Image motivation | ● | | | | | |
| | | Limited time window | | | ● | | | |
| | | Loss aversion | ● | | | YES | | ✓ |
| | | Make resources scarce | ● | | | | | |
| | | Mental accounting | ● | | | | | |
| | | Optimism and overconfidence | ● | | | YES | | ✓ |
| | | Placebos | | | ● | | | |
| | | Priming | | | ● | YES | ✓ | ✓ |
| | | Representativeness | ● | | | | | |
| | | Spotlight effect | ● | | ● | YES | ✓ | |
| | | Temptation | | | ● | | | |
| | Change choice defaults | Automatic enrolment | ● | | | | | |

| | Subcategory | Nudge | COM-B factor | | | Employed | PRE-LOG | POST-LOG |
|--|------------------------------|--|-----------------|------------------|-----------------|----------|---------|----------|
| | | | ● Capability | ● Opportunity | ● Motivation | | | |
| | | Enhancing or influencing active choosing | ● | | ● | | | |
| | | Prompted choice | ● | | ● | YES | | ✓ |
| | | Setting defaults | ● | | | | | |
| | | Simplifying active choosing | ● | | | | | |
| | Change range or composition | Change ease and convenience | ● | ● | | | | |
| | | Change financial effort | ● | ● | | | | |
| | | Change physical effort | ● | ● | | | | |
| | | Create friction | | ● | ● | YES | | ✓ |
| | | Navigability of contexts | ● | | | | | |
| | | Reduce paperwork | ● | ● | | | | |
| | | Speed bumps | ● | | | YES | | ✓ |
| | | Throttle mindless activity | ● | | ● | YES | | |
| | Change option-related effort | Change scale | ● | | | YES | | |
| | | Decision staging | ● | | | | | |
| | | Order effects | ● | | | YES | ✓ | ✓ |
| | | Partition of options/categories | ● | | | | | |
| | | Structure complex choices | ● | | | | | |
| | | Structure of evaluation | | | ● | | | |
| | Change option consequences | Change social consequences | | ● | ● | | | |
| | | Connect decision to benefit/cost | | | ● | YES | | ✓ |
| | | Micro-incentives | | | ● | | | |
| | Provide reminders | Remind of goal | | | ● | | | |

| | Subcategory | Nudge | COM-B factor | | | Employed | PRE-LOG | POST-LOG |
|------------------------|--------------------------------------|---|-----------------|------------------|-----------------|----------|---------|----------|
| | | | ● Capability | ● Opportunity | ● Motivation | | | |
| | | Remind of socially desirable concepts | | ● | ● | YES | ✓ | ✓ |
| | | Situated | ● | | | YES | | ✓ |
| | | Tutorial | ● | | | | | |
| | Facilitate commitment | Apprehensive | ● | | | | | |
| | | Automated | ● | | | | | |
| | | Eliciting implementation intentions | | | ● | | | |
| | | Just-in-time | ● | | | | | |
| | | Nature and consequences of own past choices | | | ● | | | |
| | | Precommitment strategy | | | ● | | | |
| | | Self-control strategies | | | ● | | | |
| | | Support public commitment | | ● | ● | | | |
| Social decision appeal | Increase reputation of the messenger | Expecting error | ● | ● | | | | |
| | | Messenger effect | | ● | | | | |
| | Provide social reference point | <i>Argumentum ad populum</i> | | ● | ● | | | |
| | | Following the herd (norms) | | ● | ● | | | |
| | | <i>Group ad populum</i> | | ● | ● | | | |
| | | Referring to opinion leader | | ● | ● | | | |
| | | Social influence (comparison) | | ● | ● | | | |
| | Instigate empathy | Instigate empathy with characters | ● | ● | ● | YES | | ✓ |
| | | Invoking feelings of reciprocity | | ● | ● | YES | | ✓ |
| | | Moral suasion | | ● | | | | |

| | Subcategory | Nudge | COM-B factor | | | Employed | PRE-LOG | POST-LOG |
|--|-------------|------------------------|-------------------------|--------------------------|-------------------------|----------|---------|----------|
| | | | <div>●</div> Capability | <div>●</div> Opportunity | <div>●</div> Motivation | | | |
| | | Positive reinforcement | <div>●</div> | <div>●</div> | | YES | | ✓ |

Overall the COM-B factor with the most nudges mapped by a significant margin was capability, followed by motivation and finally opportunity the least mechanisms mapped. At least conceptually, this suggests that it is easier to design nudges (in the digital context) that target an individual's understanding, skills, or capacity to perform certain behaviours, rather than targeting their personal motivation or social/physical environment. Although this does not really consider how effective said nudge mechanisms are individually.

4.4 Summary

Nudging is a behavioural intervention devised by Thaler and Sunstein (2008) that focuses on influencing behaviour by tweaking the choice architecture. Nudging is based on the broader philosophy of libertarian paternalism and seeks to influence behaviour with minimal impact on incentives or autonomy. The mechanisms by which nudging is applied can be split into four broad categories of decision information, decision structure, decision assistance, and social decision appeal. Each category contains various subcategories and specific nudging mechanisms. Table 4.2 mapped these nudging mechanisms to the COM-B factors they are most likely to target.

The next chapter focuses on the methodology applied by this study.

CHAPTER 5:

METHODOLOGICAL APPROACH

5.1 Introduction

The three preceding chapters focused on reviewing the literature surrounding traditional online banking security, dishonest behaviour, and the behavioural intervention of nudging. This chapter focuses on clarifying the research methodology that was employed to conduct this study.

5.2 Research Paradigm

This study employed an interpretivist research paradigm. According to Saunders, Lewis and Thornhill (2016:135-144), interpretivism is one of the major research philosophies. This paradigm emphasises subjectivity by focusing on the different social, cultural, and geographical contexts in which different phenomena may occur (Saunders et al., 2016). Individuals can derive different meanings or explanations for the same phenomena within these different contexts. As a result, the insights derived from these physical phenomena can become more complex due to the variation in different contexts everyone may have relative to another person. In this study's context, different individuals may hold different opinions regarding the behaviour of the hypothetical third party in the given scenario. In other words, their social background and past experiences with online banking and fraud will influence their behaviour when they encounter an opportunity to commit online banking fraud via compromised credentials. Despite the participants going through an interview with roughly the same flow of questions, there were still a few unique responses. Even when their responses contained similar ideas, their phrasing could differ. This helped incorporate the variety in participants' social backgrounds and past experiences to some degree, without having specific questions to dig deeper into them within the interview guide. Participants could express the potential behaviour of a hypothetical third party in similar scenarios and their associated rationalisations in various ways. This flexibility was why interpretivism was selected as the research paradigm.

5.3 Approach to Theory Development

The study used an inductive approach to theory development. According to Saunders et al. (2016:144-147), an inductive approach builds or adapts a theory after analysing the data or information available. The conclusions regarding the effectiveness of nudging as an additional supplement to existing online banking security and the associated rationalisations of a hypothetical third party were only developed after analysing the primary data collected. Since the understanding of the potential applicability of nudging in online banking security was not produced from preconceived notions or tested hypotheses, a deductive approach to theory development would not have been suitable.

5.4 Research Strategy

A research strategy can be defined as a researcher's plan to help achieve their research goals (Saunders et al., 2016; Phair and Warren, 2021). The research strategy was a quasi-experiment with online banking users as the participants. Every participant was able to interact with all three versions of the website. Quasi-experiment refers to the lack of a perfect comparison between the two alternate website versions. Among the three versions, the Control version was as close to a neutral design (see Section 4.2) as possible to help set a baseline of the expected behaviour of a third party with access to compromised credentials. Choice architecture elements may have pushed participants towards certain actions amongst the online banking pages. Still, they are not considered nudges because they were not deliberate manipulations to alter their behaviour. This is touched upon again within Section 5.5.3 and Chapter 8.8. The PRE-LOG and POST-LOG version explored the application of nudges at various stages of using an online banking website. This was done to help explore where it could be ideal to employ nudges on an online banking website.

The study explored how participants believed a hypothetical third party would behave in the provided scenarios where they had the opportunity to commit online banking fraud. The study also sought to explore the potential rationalisations that participants believed the third party in the scenario could use to explain or justify their behaviour. Questions were included in the interview guide, as discussed and illustrated in Section 5.5.2.2 and Appendix C. As such, the research strategy employed was based on

collecting cross-sectional qualitative data from online banking users through semi-structured interviews and participant observation. The data was cross-sectional as there were no follow-up interviews with the same participants, each participant was only taken through the interview process once, and their responses were analysed after to help understand how they believed the third party would behave and rationalise their actions.

In terms of the validity of such an approach, i.e. how appropriate was this research strategy in generating findings that could be applied (generalised) to the real world (Saunders et al., 2016: 202), a follow-up question was asked when the researcher heard an unusual or an unclear response. This was not the perfect solution to ensure the credibility of participant responses. Again, the closest thing to a follow-up interview was the short debrief, where their responses to previous questions were confirmed or clarified. At the same time, vetting participants beforehand was also beyond the scope and budget of this study and its limited resources. The best that could be managed was to rely on the pre-set criteria set on the research support sites when the project was advertised to potential participants. This also affects the authenticity, i.e. who was allowed to participate and how their views were accurately captured, see Section 5.5.2 for more detail on how they were selected and why the selection criteria in question were set.

In terms of the transferability of this study's findings, i.e. how well they could be applied to other studies and contexts (Saunders et al., 2016: 206), there has been an attempt to clarify the methodology and the instrument design employed in this study (see Section 5.5.3), but this was a summary of the key information rather than an exact step by step recreation. Time had to be taken to devise potential questions for the interview considering the study's research goals, as well as study existing online banking websites and devise ways to change the architecture to incorporate the various nudging mechanisms. Appendix A and Table B1, and Table B2 in Appendix B can hopefully give others an idea of how to apply a similar approach to other contexts besides online banking.

Whilst the research strategy did undergo a few revisions as the study was carried out, the final approach taken is described in the other sections of this chapter. Chapter 6 and Chapter 7 clarify how the data collected and analysed helped answer the original research questions of the study. Thus helping address the final validity criteria of dependability (Saunders et al., 2016: 206).

5.5 Data Collection and Analysis

The secondary data were collected via keyword searches on several academic databases. These keyword searches were used to explore the subject matter of the study and to draft the literature review chapters (see Chapters 2, 3, and 4). Section 5.5.1 of this chapter goes into more detail regarding the secondary data.

In terms of primary data collection, a qualitative approach was used that involved semi-structured interviews. Interviews were recorded, transcribed, and analysed using thematic analysis. The participants' interactions with the three versions of the website (Control, PRE-LOG, and POST-LOG) were also recorded and used to supplement the thematic analysis of the interview transcripts. Section 5.5.2 provides some extra detail regarding the primary data.

5.5.1 Secondary Data

Secondary data were primarily used in the literature review chapters (see Chapters 2, 3, and 4). The study employed a keyword search to explore the available literature, and backward searching was also used to help build an understanding of the various topics. The literature review was split into three chapters, each with a different topic. Both academic databases and a few pieces of grey literature were used.

The keyword search was similar to the process used in a scoping review; however, it did not include all the formal elements that typically comprise such a review. The keyword search was facilitated by the use of the software package Harzing's "Publish or Perish" and Google Scholar. The keywords were used to search for potentially relevant literature; the links included in the search results were used to source the full articles from academic databases. Inclusion or exclusion was primarily decided after reading the title and the abstracts of the papers found in the keyword search to determine their relevance to the study. Table 5.1 highlights some of the keywords that were used to find literature. Backward searching was also employed to find additional articles, as some relevant articles were referenced in the identified literature but did not appear in the normal keyword search results. The academic databases included JSTOR, Elsevier, ACM Digital Library, Taylor and Francis Online, SAGE Journals, UNISEX, SpringerLink, AIS E-library, IEEE Xplore, SSRN, Oxford Academic, Emerald Insight, and Semantic Scholar. As stated above, not all sources found in the searches

were obtainable from academic databases (i.e., some came from grey literature such as websites or blogs).

Table 5.1: Example of keywords used

| Online banking | Online banking security | Behaviour and (dis)honesty | Nudging |
|-----------------------------|---|--------------------------------------|------------------------------------|
| "Online Banking" | "Fraud Prevention" AND Banking | Dishonesty AND "Behaviour" | Nudging |
| "Internet Banking" | "Fraud Prevention" AND Online Banking | "Civic Honesty" | Nudging AND Banking |
| "Online Banking History" | "Two-Factor Authentication" AND Banking | Cheating AND Behaviour | "Choice Architecture" |
| "Online Banking Adoption" | "2FA Adoption" AND Banking | Dishonesty AND Rationalisation | Nudging AND Security |
| "Internet Banking Adoption" | "Authentication" | Theft AND Rationalisation | Nudging AND "Information Security" |
| | "Password Management" | "Fraud Triangle" | "Digital Nudging" |
| | "Compromised Credentials" | "COM-B theory" | |
| | "Online Banking AND Security" | Ethics AND "Decision Making" | |
| | | "Guilt Aversion" | |
| | | "Theory of Self-Concept Maintenance" | |

5.5.2 Primary Data

The primary data of the study were collected through semi-structured interviews. Although the participants' interactions with the website(s) were also recorded, it was not considered participant observation as these interactions were only utilised to supplement the thematic analysis. They supported the participants' responses and gave a sense of how an individual who used the site would interact with its nudges; thus helping to gauge the effectiveness of nudging in dissuading online banking fraud better (Hehman, Stoler and Freeman, 2015). The interviews and participant interactions were recorded via the Zoom "Record meeting" feature and the software MacroRecorder.²

² <https://www.macorecorder.com/mouse-recorder/>

5.5.2.1 Participants

Participants were recruited via the Prolific and Amazon Mechanical Turk (MTurk) research support services. These research support services help researchers recruit and remunerate participants for their research projects (O'Hear, 2019; Hillman, 2022). The participants are remunerated at a fixed rate set by the researcher when the study is advertised on Prolific or MTurk. In this case, the participants were paid £7.50/hour for participating in an interview. The average length of these interviews was 30 to 35 minutes. The sample size was kept relatively small ($n=15$), given the time-consuming nature of conducting multiple interviews, the cost implications, and the relatively homogenous population of online banking users (McLeod, 2014; Boddy, 2016; Saunders et al., 2016:297,414-416).

Participants were selected using convenience sampling for similar reasons to the limited sample size (Jager, Putnick and Bornstein, 2017). Convenience sampling is a non-probabilistic sampling technique where individuals meeting pre-set criteria are recruited based on how easily they can be reached or accessed by a researcher (Alkassim and Tran, 2016; Saunders et al., 2016:304). Individuals meeting the selection criteria (USA, 21+ years, English fluency, and online banking users) could apply to participate in the study. It is worth mentioning that there is more to the age requirement. The sample was stratified into three age groups: young (21-39 years), middle (40-59 years), and senior (60 years and older). While the sample was not meant to be representative of the larger population of online banking users in the USA, this was implemented to help provide the perspective of other age groups, potentially providing a better sense of the behaviour of a third party who encounters a similar scenario. The adoption of online banking is less common among older individuals (Berger and Gensler, 2007; Akhter, 2015; Alhabash et al., 2015).

The first selection criterion was tied to the participant's country of origin/residence. Participants were recruited from the USA due to its relatively low 2FA adoption rate by their banks (Horowitz, 2014; Colbert, 2019). This was specified and made clear on the Prolific job and was one of the requirements for the MTurk Human Intelligence Task (HIT). 2FA was excluded from the experiment as it could have made the opportunities for online banking fraud described in the scenarios less feasible to participants, as well as the potential accessibility and hassle issues brought up in Chapter 1.1 (Renaud,

Johnson and Ophoff, 2020; Renaud, 2021). At the same time, the relatively low rate of 2FA adoption/implementation by American banks ensured that the scenario was closer to the potential participants' typical use case or experience with online banking. With relatively low 2FA adoption, the few institutions in the USA that offered it were likely to only have it as an optional security feature for their clients. Thus the USA was a more ideal sample for this experiment as compared to other countries.

Considering the context of the study, another requirement was for the potential participants to be online banking users. If an individual applying to be a participant was not an online banking user, they were disqualified, and other potential participants were considered instead. As they had to know how to use online banking, it was reasonable to infer the participants interviewed had some degree of digital literacy. Still, this literacy may not have been equal among the whole sample. To help address this, a short tutorial was provided before the questions related to the Control version (see Appendix C) of the website were asked in the interview. This was done to help participants get comfortable using the website(s) and make the roleplay aspect employed in subsequent versions proceed much smoother (minimal assistance needed).

The USA, depending on the specific state, may have a different age of majority, but in general, they range from 18 to 21 years (McCue, 2018; Polumbo, 2019). To avoid working with minors and children, one of the study's selection criteria was that potential participants had to be 21 years old or older. Any applicant below this age threshold was disqualified.

The final selection criterion was that potential participants had to be fluent in written and spoken English. The study was conducted in English, and, as a result, individuals who did not meet this requirement were disqualified.

As previously mentioned, Prolific and MTurk were employed for participant recruitment. For Prolific, a job was posted that advertised the project. This job included details about the project, participant remuneration, and the selection criteria. A similar HIT was placed on Amazon MTurk to aid in recruiting participants for the study. Potential participants interested in learning more and potentially taking part could click the link on the Prolific page, and MTurk HIT, to be taken to a Qualtrics survey. The Qualtrics survey provided more details about the study, what exactly would be

expected from participants and clarification on what they would be consenting to if they chose to participate. As is the case with similar Information Systems research, participants had to give informed consent. The email address they provided in the Qualtrics survey was used to contact them and negotiate a time slot to conduct the interview. If the potential participant failed to respond to the invitation email after 72 hours, they were disqualified. After setting a timeslot with the participant, they were interviewed. After the interview was completed, payment would be authorised to the participant via the Prolific ID they provided in the Qualtrics survey. Participants recruited via MTurk had to provide a valid survey code before payment was authorised to their Worker ID. This survey code was revealed to a potential participant at the end of the Qualtrics survey, and they had to return to MTurk and submit it to complete the HIT.

5.5.2.2 Data Collection: Semi-Structured Interviews

As previously mentioned, the main method used to collect data was semi-structured interviews. Semi-structured interviews enable the elicitation of additional information from research participants when they respond to questions (Saunders et al., 2016:388-392). These further questions would be asked to better understand the rationalisations and behaviour of the hypothetical third party in the scenario. A structured interview would have been unsuitable because it would not have allowed these additional questions to be asked. On the other hand, unstructured interviews would have had a less logical flow.

The questions asked during the interview focused on the behaviour and rationalisations of the third party in the provided scenario when given the opportunity to commit online banking fraud and encounter the respective nudges on the fictitious website(s). Interviewer bias was controlled, as far as possible, by always conducting the interview calmly and politely. Interviewer bias refers to situations where the interviewer's preconceived notions influence how they conduct the interview and can subsequently influence participants' responses to their questions (Saunders et al., 2016: 397). Bar a few minor technical issues; the interviews were conducted smoothly.

The audio from these interviews was recorded and transcribed to collect the participants' responses to the questions asked during the interview. The interview guide is presented in Tables 5.2 to 5.5.

The interviews were conducted virtually via the Zoom conferencing software due to the vast geographical distance between the participants. During the interviews, the participants were presented and interacted with three versions of a fictitious online banking website developed for this study. The three fictitious websites were hosted locally on the computer used during the interview and shown to the participants via Zoom's "Screen share" feature. Zoom's "Allow remote control" feature enabled participants to interact with the three fictitious online banking websites.

Table 5.2: Interview guide (Control version)

| Scenario | Question | Motivation | Alignment |
|--|--|---|-----------|
| <i>"Jack/Jill Taylor was recently involved in a small car accident. They've gone to visit their local Internet café to browse the web in search of an affordable local mechanic to repair their car. Besides Jack/Jill Taylor, there isn't another customer in the café. While walking past, Jack/Jill notices one of the machines is on and has an online banking website open. Credentials are on a sticky note under the keyboard."</i> | Given what you have seen on this version of the interface, what do you think Jack/Jill would do if they encountered it along with the credentials? | Get a sense of what a third party may do if they encounter someone else's online banking credentials – establishing a baseline of behaviour, as the control version of the website is as neutral as possible. | RQ1 |
| | What would Jack/Jill's thought process (or rationalisation) be when making that decision? | Get a sense of the rationalisations that a third party may go through when they make their decision about what to do on the website. | RQ3 |

Table 5.3: Interview guide (PRE-LOG version)

| Scenario | Question | Motivation | Alignment |
|--|--|---|------------|
| <i>"While walking past, Jack/Jill notices one of the machines is on and has an online banking homepage open. Jack/Jill also notices that the online banking credentials seem to have been saved on the machine."</i> | Jack/Jill did _____! Would they also commit an unauthorised transaction? | General idea: Based on observed behaviour while the participant is roleplaying, how would a third party on the PRE-LOG page behave? Beyond using the credentials, would they go a further step and perform unauthorised transactions? | RQ1 RQ2 |
| | What was Jack/Jill's thought process or rationalisations for deciding to do that (hit login) (or transact)? | Get a sense of the rationalisations a third party may use for their behaviour. | RQ3 |
| | Going back to the homepage of the interface, what aspect(s) or feature(s) would have stood out the most to Jack/Jill? Did those aspects affect (play a role in) Jack/Jill's decision or thought process? If so, how? | Get a sense of what nudge(s) the participant may have noticed on the page and, subsequently, the potential effect they may have had on the behaviour and rationalisations of a third party. | RQ1 |

Table 5.4: Interview guide (POST-LOG version)

| Scenario | Question | Motivation | Alignment |
|--|---|---|-------------------|
| "While walking past, Jack/Jill notices one of the machines is on and has an online banking website open. Jack/Jill also notices the previous user forgot to log out of their account!" | Jack/Jill did ____! What was Jack/Jill's thought process or rationalisations for deciding to do that click (or transact)? | Observe what the participant roleplaying as the third party on the website would do on this version of the fictional online banking website. Learn what a third party is likely to do in the scenario. Also, discover some of the rationalisations a third party may use if the online banking account is open. | RQ1 RQ2 RQ3 |
| | Looking back to the pages you encountered in this POST-LOG version, would any feature(s) or aspects(s) have stood out to Jack/Jill? | Get a sense of what nudge(s) the participant may have noticed on the page and, subsequently, the potential effect they may have had on the behaviour and rationalisations of a third party. | RQ1 |

Table 5.5: Interview guide (comparison of versions)

| Question | Motivation | Alignment |
|--|---|------------|
| Looking back between the PRE-LOG and POST-LOG versions, which version could have had the more significant effect on Jack/Jill's behaviours and rationalisations? Why? | As close to a direct answer to RQ2 as we can get from the participant. It helps to get a sense of where on online banking websites it may be more effective to place some nudging mechanisms. | RQ2 RQ1 |
| If both versions (halves) were combined, how would this impact the behaviour and rationalisations of Jack/Jill? (If it makes any difference at all?) | While the project may have sought to compare and contrast nudges employed at different steps/stages, in reality, nudges may be used across the whole site. The motivation for this question is to check if this would yield additional benefits in terms of dissuading online banking fraud or if banks should instead focus on one step/stage. | RQ2 |
| Which aspect on all three versions (specifically fraud, yes) had the most effect on Jack/Jill's behaviour? | Get an idea about what may overall have been the most effective nudge employed. Subsequently, gaining a sense of which was the most effective at dissuading online banking fraud. | RQ1 |

5.5.3 Instrument Design

The fictitious bank used in this study was called Horizon Banking. The three versions of their online banking website were the Control, PRE-LOG, and POST-LOG. As evident in the interview guide, each version had its own corresponding scenario. The three versions of the website were developed using the wireframing software tool Axure RP 10.³ This tool is aimed at helping user experience professionals to build more functional prototypes for their organisations and clients (Axure Software Solutions, 2022). Axure was used to generate interactable websites that looked and functioned very similarly to the typical interface of an online banking website. The online banking websites of three South African banks and five American banks were examined. These online banking websites were examined to understand what options should be available on the interface of an online banking website. These websites served as the inspiration for designing the Control version.

The Control version represented an online banking website's interface with no deliberate choice architecture manipulations (nudges) employed on the interface. It was intended to be the version with choice architecture being as neutral as possible while being close to what the South African and American banks may use for their online services. The Control version was the first to be developed of the three versions of the website. For example, the homepage of the Control version is shown in Figure 5.1. The other parts of the alternate nudge versions, POST-LOG and PRE-LOG, were the same as the Control, i.e., Control/Control, PRE-LOG/Control, and Control/POST-LOG. The other 'half' of the nudge version of the website being the same as the Control version was to help isolate any change in behaviour of a hypothetical third party to deploying the nudges at that step (i.e. if behaviour deviated from the Control version, it could be attributed to that versions employed nudges) The two alternate versions are meant to represent the different stages in the process of committing online banking fraud. Granted, this was not a perfect comparison as the scenario design for the three versions was slightly different (see Tables 5.2, 5.3, and 5.4). At the same time, it does not take into account the differences in difficulty in implanting nudges on the two nudge versions (PRE-LOG and POST-LOG), as there is a difference in how much

³ <https://www.axure.com/>

functionality is available to users of the website. Thus affecting the degree to which nudges could be implemented for each version.

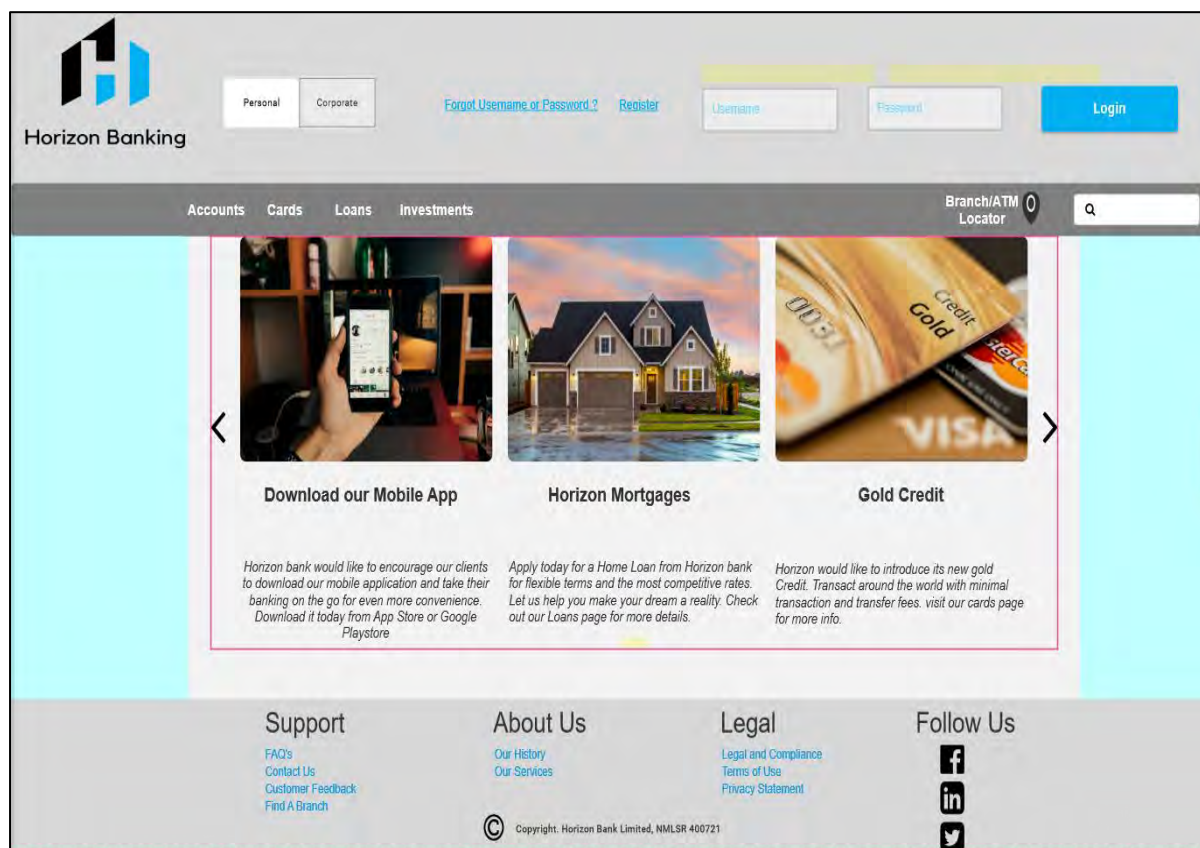


Figure 5.1: Control homepage screenshot

Once the Control version was developed, it was re-examined to determine the potential aspects of its choice architecture that could be modified to incorporate some of the nudge mechanisms from Chapter 4.3 and to create the two alternate versions. The PRE-LOG version represents an interface with nudges employed before a user, authorised or not, logged in to an account. The implemented nudges thus aim to prevent a third party in a similar scenario from using the compromised credentials in the first place, i.e., to prevent online banking fraud at the earlier steps in the process. The POST-LOG focused on employing nudges after the user, authorised or not, was already logged in and had access to the online banking account. Its accompanying scenario was designed to reflect the third party now having the opportunity to exploit their unauthorised access to conduct transactions and enrich themselves. The nudges implemented on this version (i.e., after logging in) were designed to dissuade an individual from completing the last steps in the process of committing online banking

fraud. Overall the separate nudge versions were designed to help compare where deploying nudges may be more effective and thus deal with the second research question (RQ2).

The homepage of the PRE-LOG version is used as an example in Figures 5.2 and 5.3. The full catalogue of screenshots and nudges employed on the interfaces of the three versions of the website is included in Appendix B.

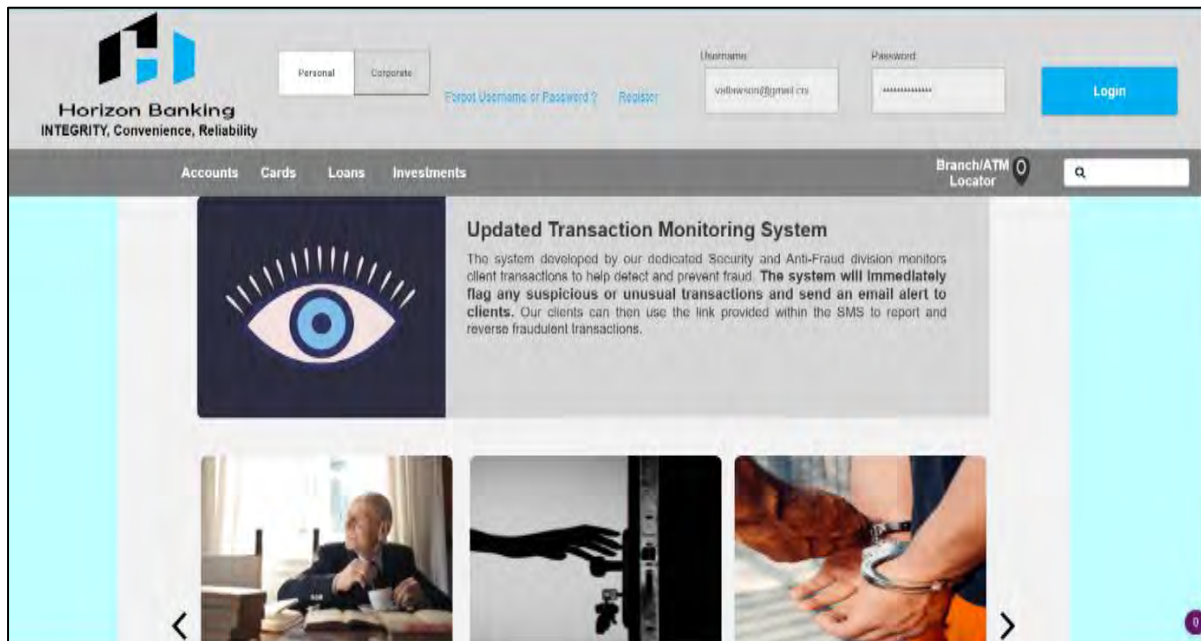


Figure 5.2: PRE-LOG homepage top

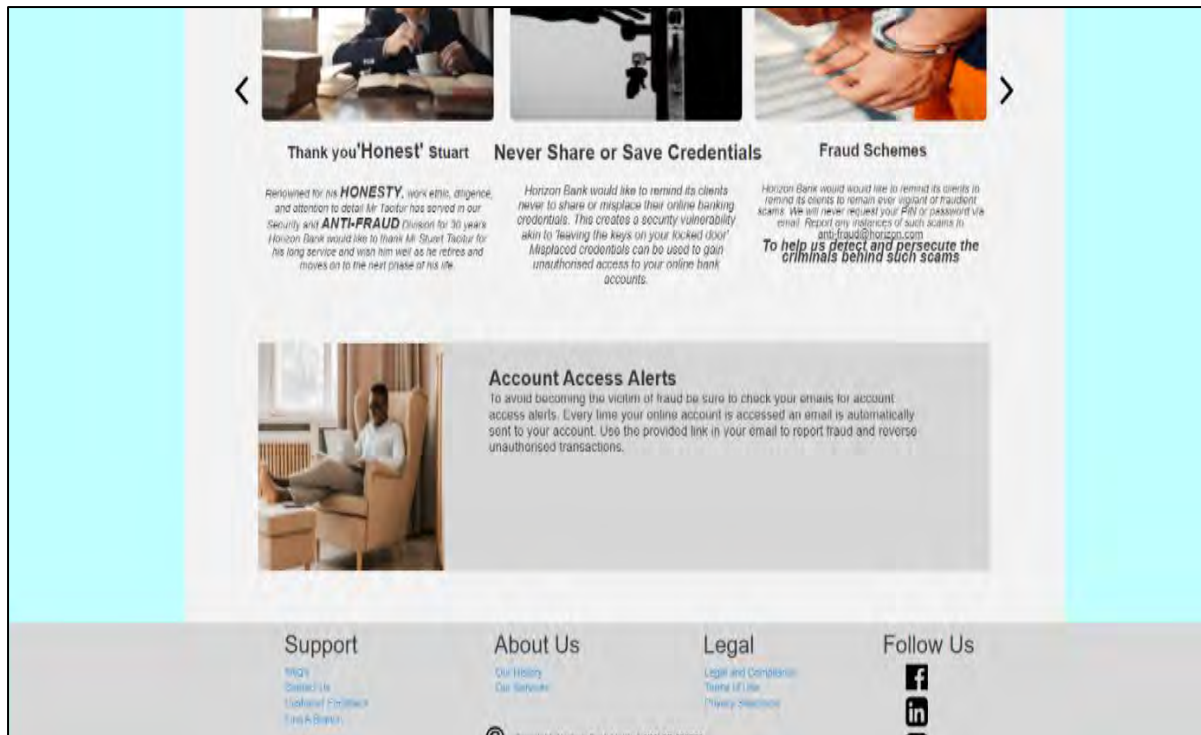


Figure 5.3: PRE-LOG homepage bottom

The focus of this study was the functionality of viewing the online banking account, adding a recipient, and paying that recipient from the available funds. In other words, an unauthorised transaction while using the online banking website. Figure E1 in Appendix E is an Entity Relationships Diagram (ERD) used to model a limited version of the hypothetical database of Horizon Banking. The entities included in an ERD for online banking could be more numerous, but they were excluded to focus on the login, viewing account data, adding recipients, and making payments. The Hierarchical Task Analysis (HTA) diagrams included in Figures E4 and E5 in Appendix E are meant to model and break down the various tasks users can perform when they visit an online banking website. The latter HTA diagram in Appendix E (see Figure E4) was a task breakdown intended to reflect the focus of this study. Logging in and making a payment were also modelled using behavioural state machines. They are included in Figures E2 and E3 in Appendix E. The former outlines the login and credential validation processes employed on the bank's websites. The latter was used to design the various steps used within the interfaces for making a payment.

Together, the ERD, HTAs, and Behavioural State Machine diagrams are meant to clarify the tasks and processes a user could complete on the interface. These were

designed to examine the online banking websites mentioned earlier. They subsequently helped to inform the design of the three websites created for this study.

Across all versions, not every aspect of the UI was fully functional; some elements were left on the website for decorative purposes. They were part of a “normal” online banking website but were not necessarily part of the focus of the study and were thus left inactive/non-functional. An example of the investments link in the global navigation on the PRE-LOG homepage is provided. This is shown in Figures 5.4 and 5.5. To help participants avoid these inactive and decorative parts of the website, they were briefed about them at the start of the interview. The tooltip “Interaction DISABLED” was shown when the mouse hovered over them.

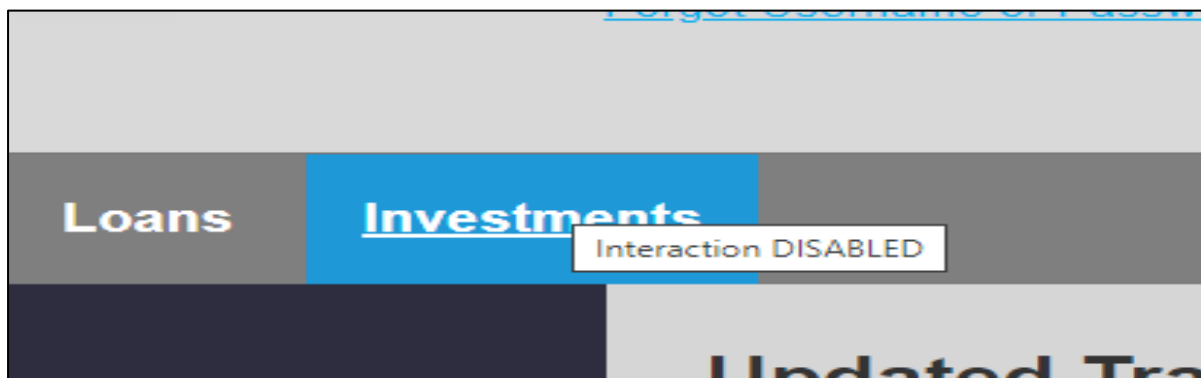
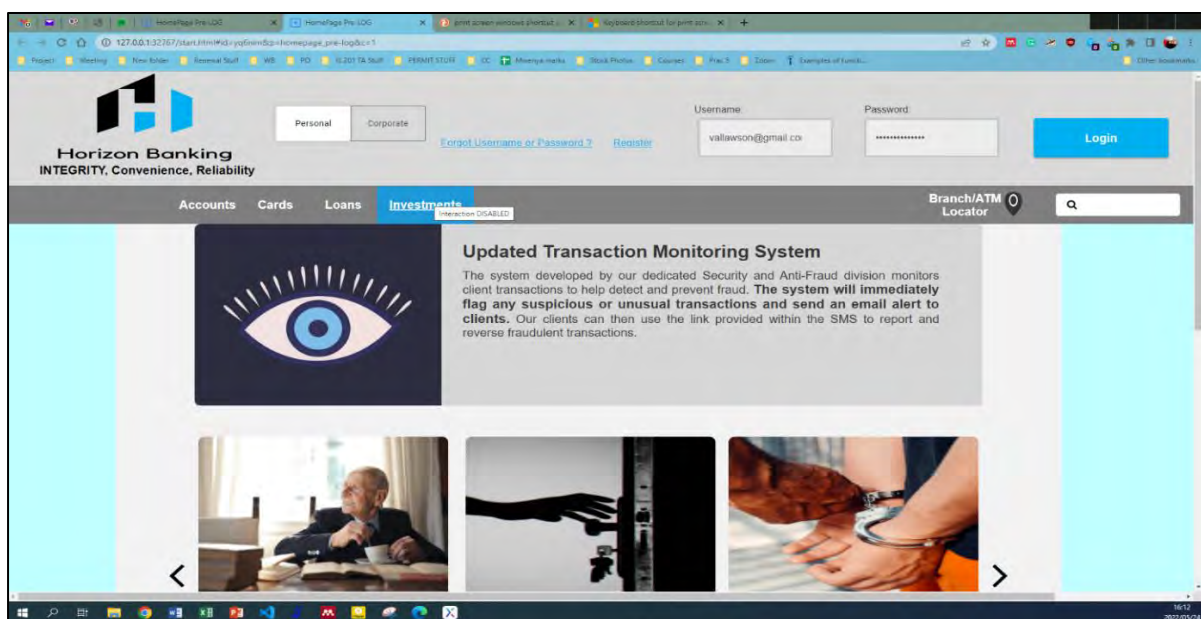


Figure 5.4: Interaction DISABLED screenshot cropped



5.5.4 Data Analysis

The interview transcripts were analysed using thematic analysis. Thematic analysis focuses on grouping ideas and concepts found in qualitative data by formulating codes (Saunders et al., 2016:579-588). This data-analysis method was appropriate due to the qualitative nature of the data and the nominal variation in the responses from the participants who were interviewed. It was used to look deeper at all the participants' responses and to find common ideas and themes regarding how a hypothetical third party in the scenario could behave and rationalise their behaviour and decisions. The analysis was conducted using the NVivo QSR International software. The study employed the six-phase thematic analysis process as described by Braun and Clarke (2006) (additional details are provided in Section 6.4).

In the paper on their process, Braun and Clarke (2006) describe a few key terms: the data corpus, the data set, the data item, and the data extract. The data corpus is all data collected for a particular study, while a data set refers to all the data used for a particular analysis. In the context of this study, the data corpus is the secondary data, the observations recorded, and the interview transcripts. The analysed interview transcripts would be the primary data set used for the thematic analysis, as described later. A data item is an individual piece of the data collected that forms part of the data set. In this context, this would refer to a single transcript. A data extract refers to an individual piece of coded data extracted from a data item. In this study's context, a single interview transcript would be an example of a data item, while the responses extracted from these transcripts would be examples of data extracts.

The first phase involves familiarising oneself with the data (Braun and Clarke, 2006). In the context of this study, this meant listening to the audio recordings of the interviews and manually transcribing the data. The transcripts are the data set used in the later analysis phases.

The second phase of the process involved generating an initial list of codes from the data set (Braun and Clarke, 2006). This phase involved going through the data set and sorting interesting observations and statements from participants' responses into

various codes. The product of this phase is the full list of codes and the project map visualisations.

The third phase of thematic analysis involved grouping or sorting the various codes into broader themes (Braun and Clarke, 2006). Each theme generally referred to a common idea expressed by the participants during the interviews. The codes were reviewed before grouping them into initial themes. The initial themes were primarily data driven or inductive, as they arose from a common idea found in the codes. For example, Figure 5.6 provides a compressed version of an initial thematic map (NB: the full version can be found in Appendix D with the other mind maps).

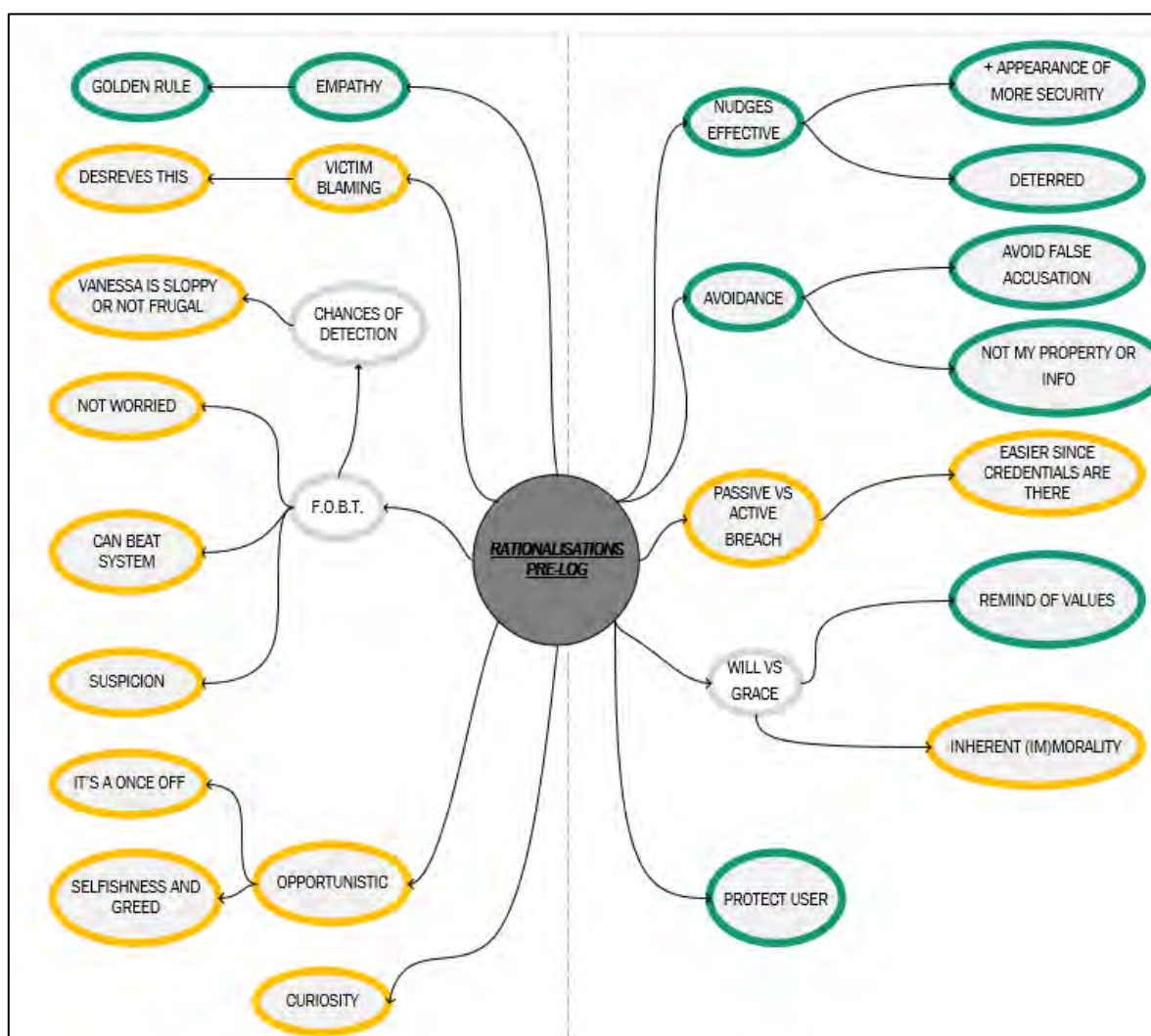


Figure 5.6: An initial thematic map for the PRE-LOG version rationalisations

The list of initial themes was then used as the primary input in the fourth phase. This phase focused on reviewing and refining the themes (Braun and Clarke, 2006). The

initial group of themes shrank in size throughout this phase as some themes were merged with other themes due to their similarities. The refined themes were then used to produce this phase's main product, namely the initial thematic (mind) maps. The thematic map represents the refined themes and how they may relate to other themes and codes. All mind maps were initially generated in NVivo, but they were subsequently recreated in the software package Microsoft Visio to look more presentable.

The penultimate phase of thematic analysis involved further refining the themes from the initial thematic map and writing detailed descriptions of each theme (Braun and Clarke, 2006). Each theme was then reconsidered in terms of what it revealed about the “bigger picture”. The number of themes shrank further after the refinement. The product of this phase was a set of core themes and subthemes that captured all the main findings from the data. These core themes were then used to produce a final thematic map.

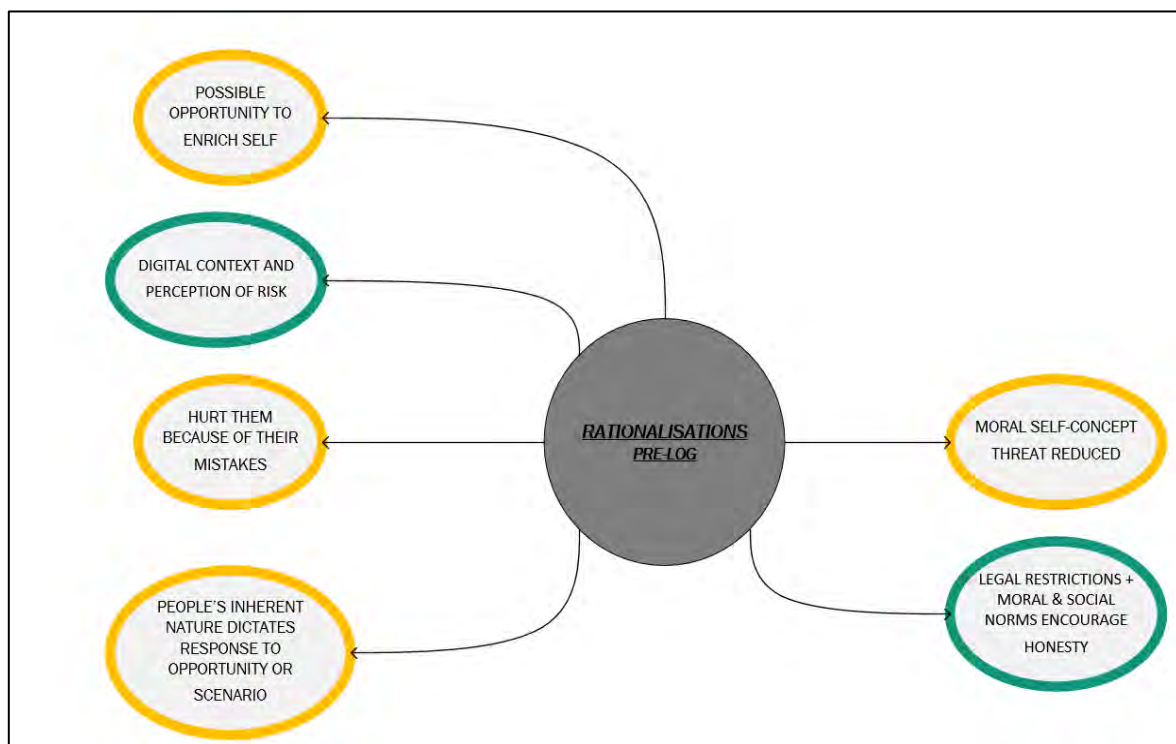


Figure 5.7: A refined thematic map for the PRE-LOG version rationalisations

The final phase of the analysis involved taking the “core” themes and final thematic map to generate a write-up of the findings and discussion chapters in general. More

detail and the results of this analysis are provided in the findings and discussion chapters (see Chapters 6 and 7).

5.6 Summary

This chapter outlined the methodological approach used by the study. This multi-method qualitative study employed the interpretivist research paradigm and used inductive reasoning. Secondary data for the literature review chapter were collected through a keyword search facilitated by Harzing's Publish or Perish and Google Scholar, as well as backward searching. Primary data for this project were collected via semi-structured virtual interviews on Zoom and participant observation. During the interview, the participants were given the opportunity to interact with three versions of a fictitious online banking website. These websites formed the research instrument, and their design was based on other South African and American banks. The next chapter examines the findings discovered after analysing the primary data gathered.

CHAPTER 6:

FINDINGS AND ANALYSIS

6.1 Introduction

The previous chapter focused on explaining the methodology employed by this study. This chapter focuses on analysing the primary data gathered for the study and describing the findings. These findings were meant to help answer the original research questions from Chapter 1. Thematic analysis was used to analyse the collected data, especially regarding the participants' rationalisations.

6.2 Sample Demographics

As mentioned in the previous chapter, participants were recruited via Amazon MTurk and Prolific. They had to be over the age of 21, live in the USA, be fluent in English, and be online banking users. At the end of the recruitment and data-collection phase, 15 participants matching these criteria were recruited and interviewed for this study. Regarding demographics, only three variables were collected, namely gender, age, and educational background.

As Table 6.1 illustrates, the study had a relatively well-balanced sample in terms of the gender of participants, with eight males and seven females. As mentioned in the previous chapter, the sample was stratified into three groups, namely young (Group A), middle (Group B), and senior (Group C). Young represented participants 21 to 40 years old, middle represented participants 41 to 59 years old, and senior represented participants 60 years or older (Akhter, 2015; Alhabash et al., 2015; Gatsou, Politis and Zevgolis, 2017; Kumari, 2017). Each group was equal in size, and all but the senior group skewed towards a gender distribution with more males. The oldest participant in the study was a 75-year-old female, while the youngest was a 30-year-old female. Table 6.1 also indicates the education demographics of these groups. This described the participants' highest level of academic achievement reached. Overall, the entire sample had reached at least a tertiary level of education. Most participants held a bachelor's qualification.

Table 6.1: Sample demographics (n=15)

| Demographics | Group A (21-39 years) | Group B (40-59 years) | Group C (60+ years) |
|------------------------|--------------------------|--------------------------|------------------------|
| Number of participants | 5 | 5 | 5 |
| Gender | | | |
| Male | 3 | 3 | 2 |
| Female | 2 | 2 | 3 |
| Education | | | |
| Associate's degree | 2 | - | 1 |
| Some college | 1 | 1 | - |
| Bachelor's degree | 1 | 2 | 3 |
| Some graduate studies | - | 1 | - |
| Master's degree | 1 | 1 | 1 |

6.3 Most Effective Nudges

This section focuses on the findings regarding the impact of the nudges. The more impactful a nudge was, the more likely it was to be effective in dissuading online banking fraud. The participants were asked what aspect of the website may have stood out the most to Jack/Jill for both the PRE-LOG and POST-LOG versions. The goal of these questions and the follow-ups that may have been asked was to get a sense of which nudges the participants, or the average third party, may have consciously noticed. Effectiveness in this context refers to how well the nudge(s) could alter the behaviour of a third party and ideally dissuade them from committing online banking fraud. The findings in this section are therefore aligned with the first research question:

RQ1: Which choice architecture manipulations (“nudges”) are the most effective at dissuading online banking fraud?

After analysing the transcripts, the relevant extracts were coded under SIGNIFICANT (PRE), SIGNIFICANT (POST), and SIGNIFICANT (General). “General” refers to the extracts that compared the most effective nudges across all three versions. The three codes were analysed to help track the most effective nudge and generate mind maps. Some respondents mentioned multiple aspects of the page; some nodes thus had child nodes. For example, “Updated transaction monitoring system (TMS)” and “+ handcuffs” meant that a participant mentioned both the Updated TMS message and the handcuffs.

6.3.1 PRE-LOG Version

The mind map for the PRE-LOG version and its most effective nudges is shown in Figure 6.1. This mind map illustrates the various ideas and concepts discovered when analysing participants' responses to the questions regarding what stood out on the website.

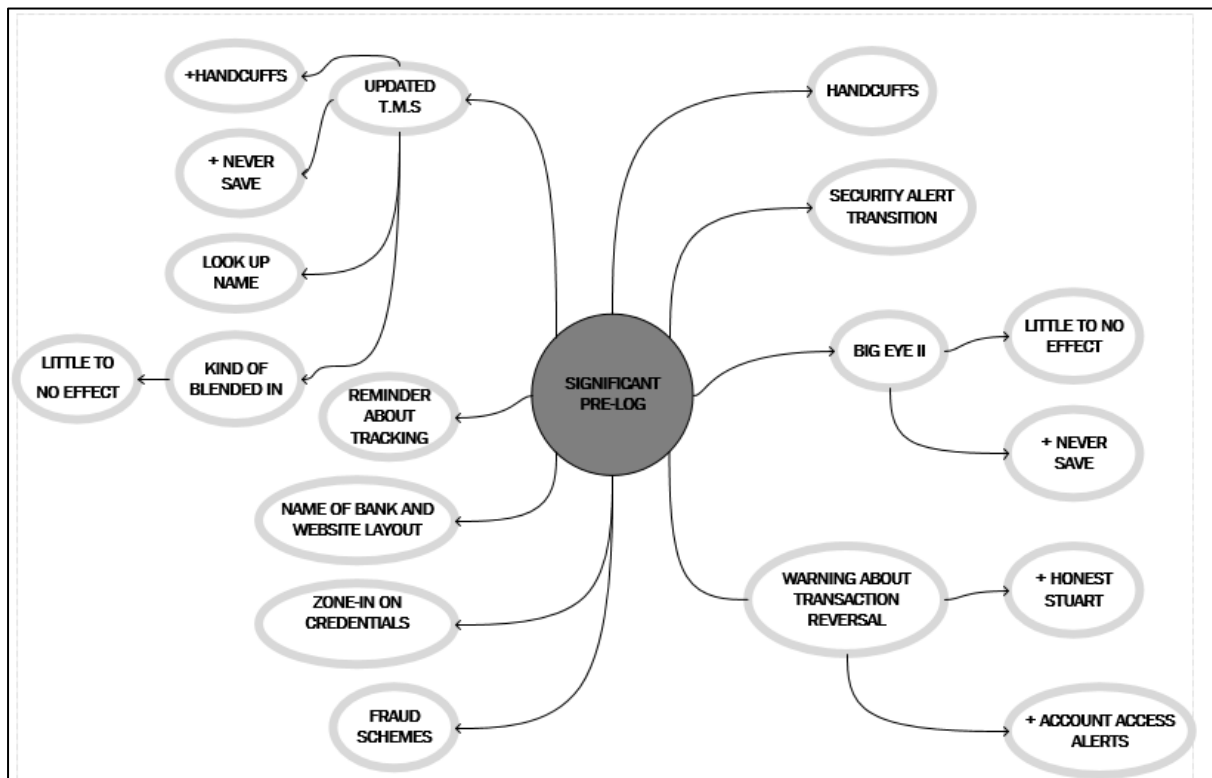


Figure 6.1: PRE-LOG version SIGNIFICANT nudges mind map

Based on the participants' responses, the three most effective aspects of the PRE-LOG version's choice architecture listed in order were:

1. Updated TMS

"P1: Hmm, I think. maybe like where it says that the, umm, updated transaction monitoring system for anti-fraud. Like she might be concerned with that. If you were to login. Maybe they'd find out that she might have something to do with that."

R: "So, Jill would be worried about being traced or detected?"

P1: "Yeah, I feel like they'd somehow find out like by tracing her."

Participant 1 (Female, 32, Associate's Degree)

2. The handcuffs

P14: "The fraud scheme immediately just stood out because visually with the handcuffs, you know. It just drew my attention. I think it would others..."

Participant 14 (Male, 45, Some College)

3. The big eye

R: "Okay. So, I'm now going to share the PRE-LOG version. You can see my screen."

P10: "Yes, with a big eye on it."

R: "Yeah. So, you've already mentioned the eye. Would the average person also notice that when they visited this version?"

P10: "They would have had to. That's the first thing I saw. Very obvious."

Participant 10 (Female, 75, Associate's Degree)

Of the three, the "Updated TMS" page was the most common aspect of the page mentioned by the respondents to a very significant degree. While the handcuffs are ranked second in the list above, there was another code worth noting, namely "Zone in". This code refers to responses that suggest that the first and often only thing a participant or third party may have noticed would be the credentials. In terms of the participants' responses, this arose more often than the mention of the handcuffs on the PRE-LOG version but was technically not an aspect of the website.

R: "Okay, so in terms of the rationalisations, that pretty much covers it. So, I noticed that it's sort of like zoning in, and so would like Jill actually explore the homepage? Or would she literally see the credentials on the site and hit the login?"

P3: "I feel like she would just see the login. I don't think she would spend too much time on the homepage. They should just zone in."

Participant 3 (Female, 30, Bachelor's Degree)

R: "Okay. And, yeah, that's pretty, so it was a similar sort of thought process and then thinking back to that homepage, would an average person have noticed anything about the page?"

P14: "Not especially, other than the fact that there were credentials in the form fields."

R: "Okay, and so they would have only really noticed the credentials?"

P14: "Yeah."

Participant 14 (Male, 45, Some College)

This response suggests that some third parties may (initially) ignore most of the website and focus only on using the credentials to gain unauthorised access to the online banking account. This potentially ties into the opportunism aspect of the rationalisations noted in Section 6.5.9.

6.3.2 POST-LOG Version

The mind map for the POST-LOG version and its most effective nudges is shown in Figure 6.2. The 10 nodes represent the various responses provided by the participants.

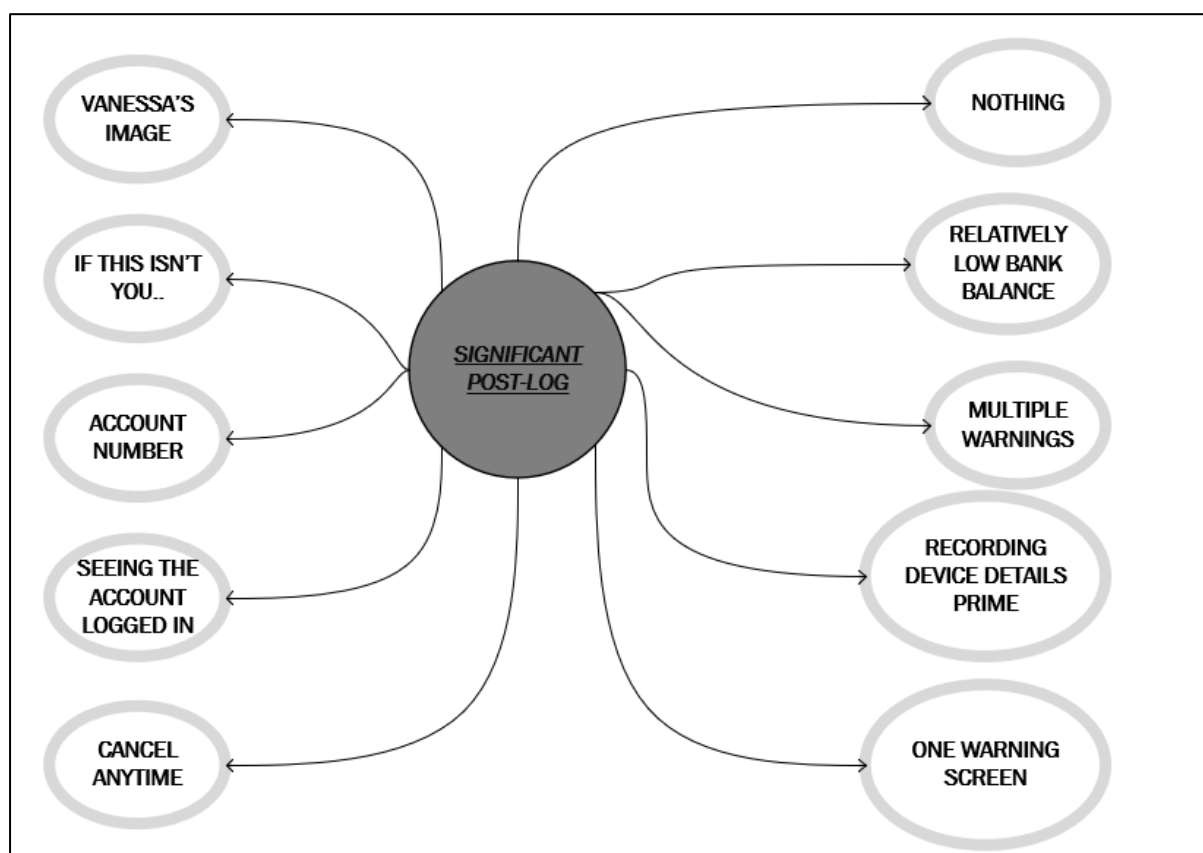


Figure 6.2: POST-LOG version SIGNIFICANT nudges mind map

Based on participants' responses, the two most prominent aspects of the POST-LOG page were:

1. Vanessa's image

P3: "So I think that seeing the picture here makes it like very personal, and I think that this person in the scenario would feel very bad about like tampering with any information here. With this, with two large pictures staring at you and she's obviously an older woman. She's smiling. She seems friendly, so

I would probably log out in this case or hit 'If this isn't you, click here', so I probably do the same thing. I mean, do the right thing here. Hit click here."

Participant 3 (Female, 30, Bachelor's Degree)

2. The link "If this isn't you, please click here."

R: "You've already mentioned the 'If this isn't you, please click here'. So that is the only thing that really stands out?"

P14: "Oh, yeah, I think that's the only thing that looked unusual. I've never... you know, you rarely see that. If you're on a public machine, you know, do X; if not, do Y. Yeah, normally, I would just hit the log out but since there was a, but literally spelling out what I was [sic]. You know it's not me. I guess I'll click here."

Participant 14 (Male, 45, Some College)

There were other responses regarding the effective aspects of the POST-LOG version's choice architecture, but the two mentioned above were the most effective by a significant margin. While the other eight nodes were relatively unique, they were not repeated often enough among participant responses to note.

6.3.3 Across All Three Versions

The final SIGNIFICANT mind map in Figure 6.3 focused on an overall comparison of the most effective nudge across all three versions of the website. This is a more direct answer to the first research question and, overall, the image of Vanessa from the POST-LOG version arose as the most effective nudge across all three versions.

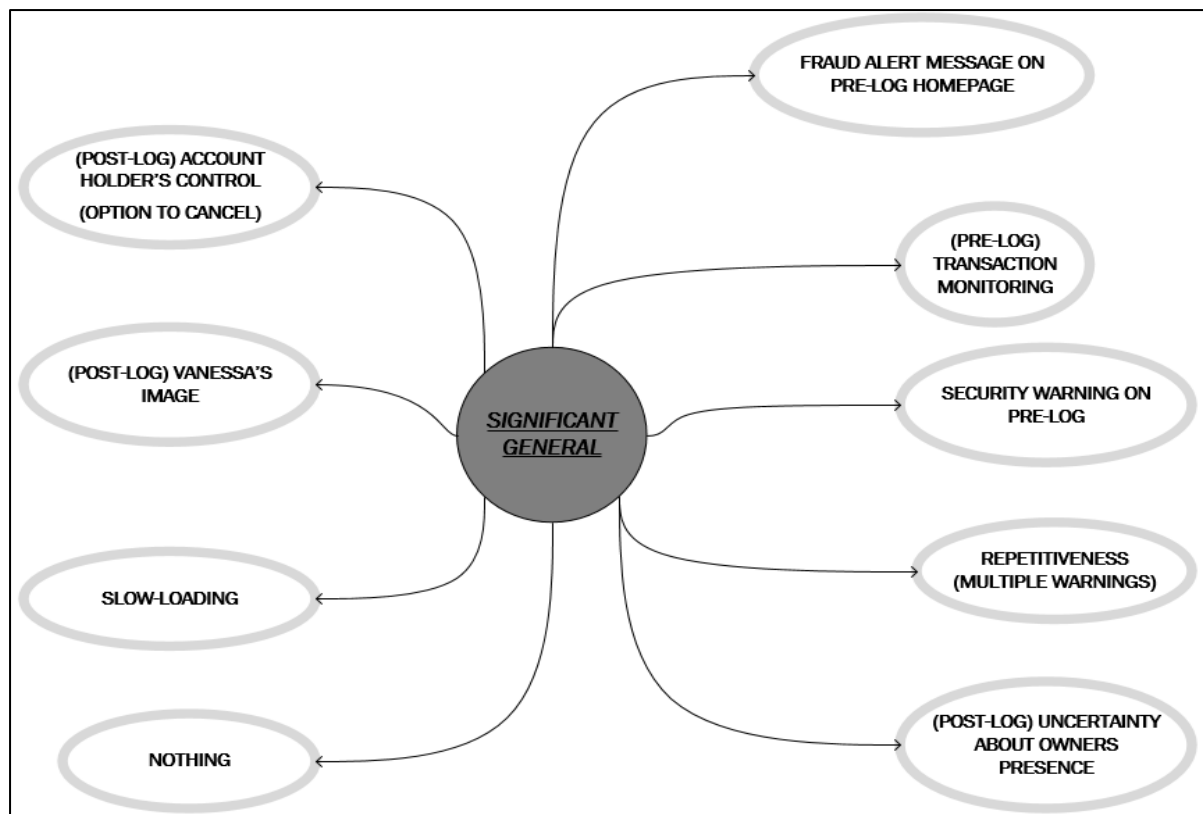


Figure 6.3: General SIGNIFICANT nudges mind map

6.4 PRE-LOG vs POST-LOG Effectiveness Comparison

This section focuses on summarising the behaviour of the participants interviewed for the study. Behaviour refers to how participants interacted with the three versions of the website and their responses to the relevant interview questions. This gave a sense of what a third party in a similar scenario might do. Some coding was employed here but not the full thematic analysis process described by Braun and Clarke (2006). For Phase 2, based on the transcripts and recorded observations, codes were generated to gain a sense of what a hypothetical third party would do in the scenario. These observations and codes were used to draw up tables to summarise and compare the overall responses and observations. These tables made it easier to track each participant's responses to the three versions and compare their effectiveness in dissuading online banking fraud. The end goal was to help determine where deploying nudges would be more effective. The findings in this section are thus aligned with the second research question:

RQ2: When comparing the placement of nudges before and after logging in, where is it more effective to deploy nudging to dissuade online banking fraud?

6.4.1 Overall Impression of More Likely Behaviour(s)

In terms of behaviour, it was not always clear-cut whether a third party would commit online banking fraud. In other words, the participants did not always give a definite yes or no response regarding whether a third party would commit online banking fraud. Some participants provided different versions of a third party in response to the questions posed to them, i.e., “normal Jack” or “criminal Jack”. Other responses gauged the likely behaviour of the average third party in the scenario(s) as a percentage.

P12: “So again, I’m going to go and put a number to it, 25%, that’s... or the people that would actually do something.”

Participant 12 (Male, 33, Master’s Degree)

P5: “So I’m going to give you two answers. I think the normal Jack would log this out for the user. I think a criminal Jack would do the exact same thing. Record this account number. And now that we’ve got a photograph, I think he might try and research her on Facebook or any of the social media to...”

Participant 5 (Male, 47, Bachelor’s Degree)

As a result, some participants’ responses were a mix of a third party behaving dishonestly (committing online banking fraud) and honestly (not committing online banking fraud in the form of transacting or tampering with settings of the online banking account). The final classification of the responses was based on the overall impression they gave regarding which behaviour was more likely to occur.

For each version of the website, after the participants were given the opportunity to interact with the website, they were asked what they thought Jack/Jill would have done in the scenarios described in the interview guide(s) (see Tables 5.2 to 5.5) discussed in Section 5.5.2.

Figure 6.4 summarises the overall impressions gleaned from the participants’ responses to these questions, as well as their recorded interactions, on what a third party in such a scenario would likely do. “Honest” represents an overall response that suggests that a third party probably would not end up committing online banking fraud. “Transact” represents responses that suggest that a third party would commit online banking fraud by transacting or tampering with an account. “Mixed” represents the exceptional situations where it was not apparent which version of a hypothetical third

party was the more likely to occur in the scenarios described. The instances where third parties may log in but not transact are still considered honest because it was relatively common for curiosity to lead to exploration. In other words, a third party may be curious and explore the account, but they do not perform an unauthorised transaction or tamper with the account.

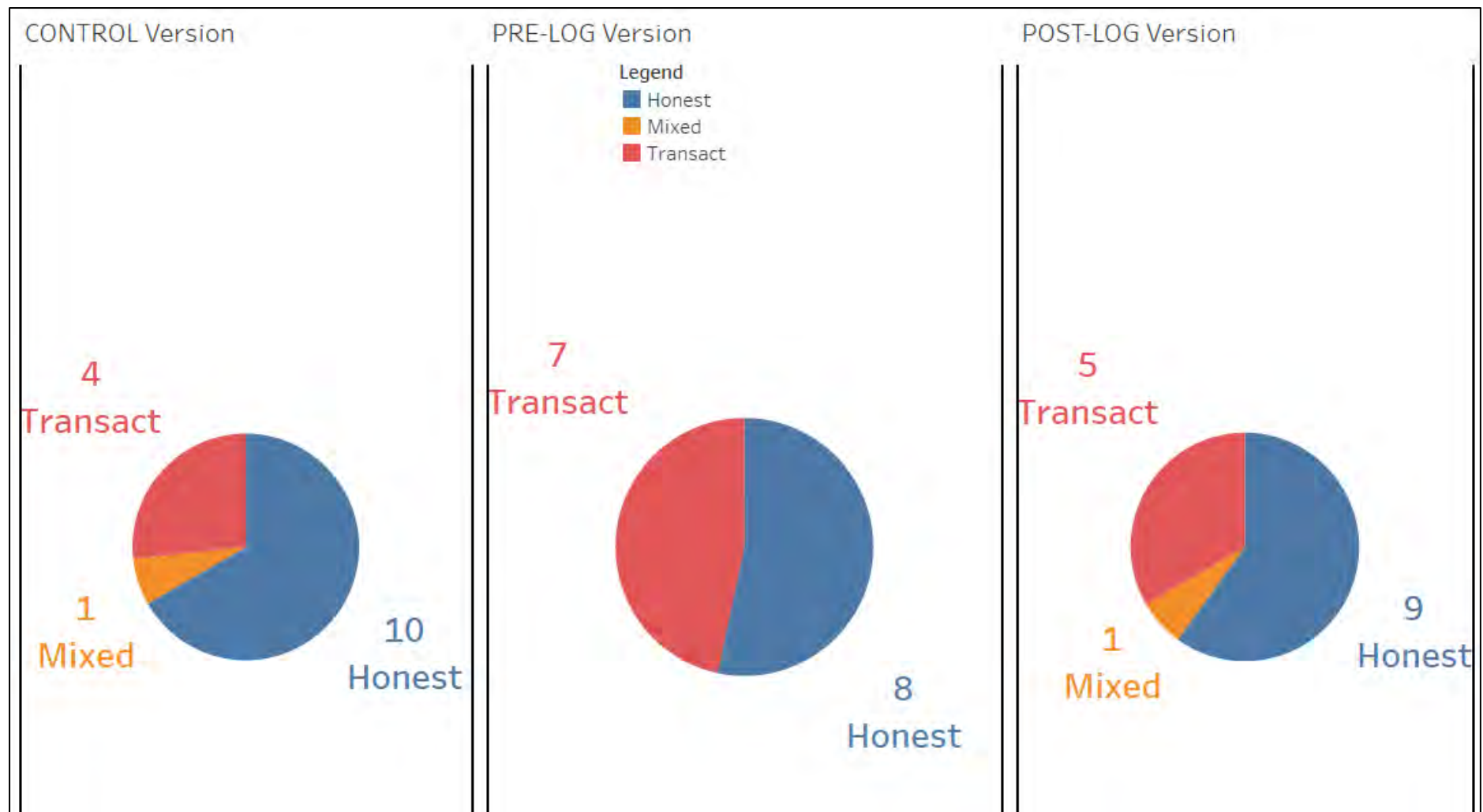


Figure 6.4: Behaviour of hypothetical third parties in the scenario(s)

Across all three versions, the suggestion was that a hypothetical third party in the scenario(s) was more likely to behave honestly than commit online banking fraud. With the exception of the PRE-LOG version, a third party was much more likely to behave honestly in the scenario(s). The PRE-LOG version was much closer to an even split in terms of how likely a third party would behave honestly or dishonestly in the provided scenario(s). Despite the Control version having minimal nudges employed to remain as neutral as possible, the PRE-LOG version had a higher likelihood of online banking fraud being committed by a third party. A possible cause for this is discussed further in Section 7.4.

6.4.2 Comparisons of the PRE-LOG and POST-LOG Versions

Figure 6.5 focuses on visually summarising the direct comparison of the effectiveness of PRE-LOG and POST-LOG versions, as well as how combining the two might affect the website's overall effectiveness in terms of dissuading online banking fraud. Most participants' responses suggested that the POST-LOG version was more effective than the PRE-LOG version in dissuading online banking fraud. At the same time, in terms of combining the PRE-LOG and POST-LOG versions, the majority of responses also suggested that such a combination would yield no additional benefit in terms of effectiveness in dissuading online banking fraud. Overall, these findings suggest that the ideal place to deploy nudges is after the online banking user has logged in. No significant or unusual trends were revealed when filtering by demographic factors. This suggests that the effectiveness of nudging on online banking websites is not impacted by the education, age, or gender of the individual(s) being targeted.

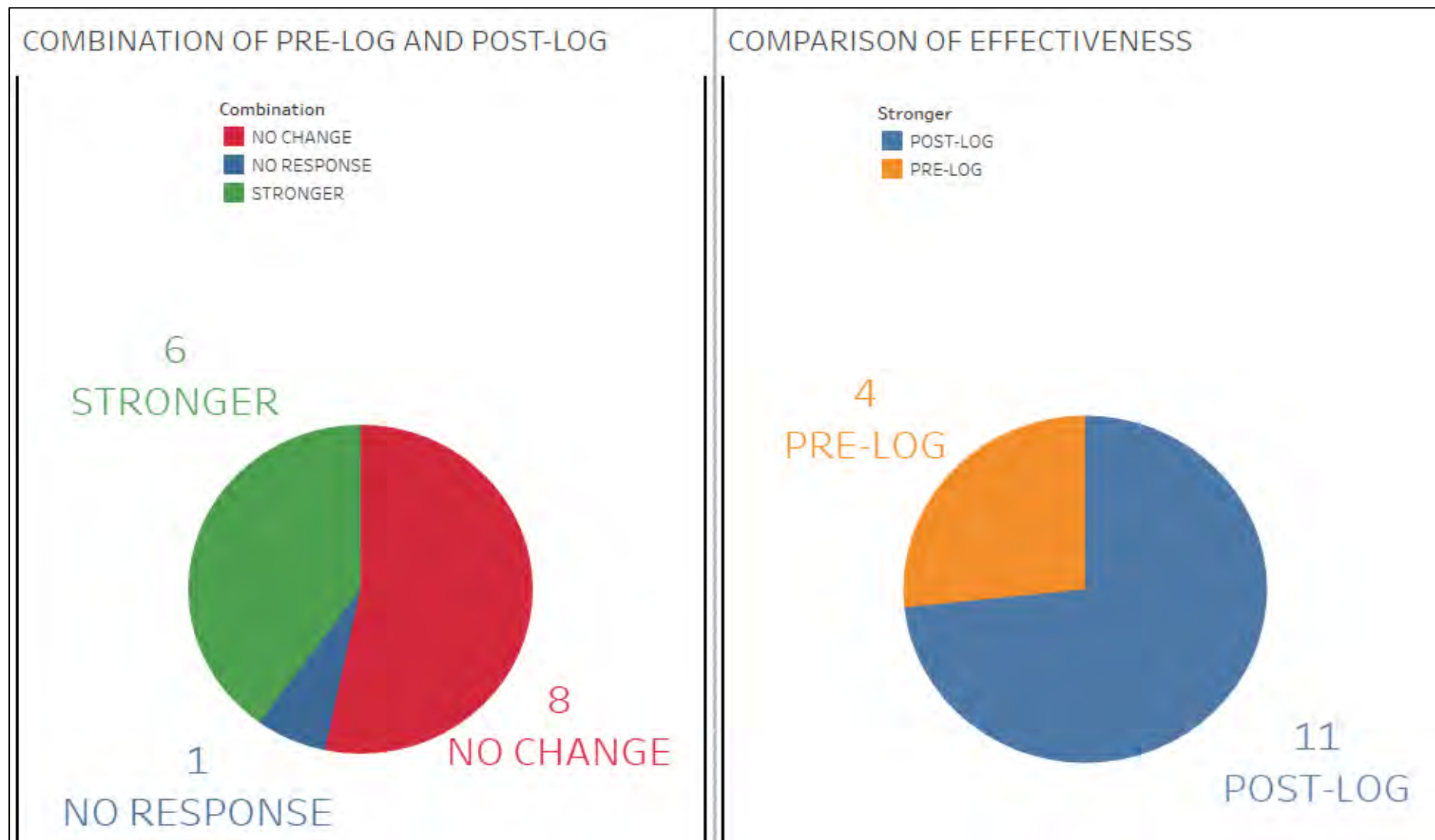


Figure 6.5: Comparison and combination of PRE-LOG and POST-LOG

6.5 Participant Rationalisations

This section's findings align with the third and final research question from Chapter 1 as it focuses on the rationalisations provided by the participants during the interviews:

RQ3: If a third party impersonates or defrauds the legitimate account holder, how do these individuals rationalise their dishonest actions?

To help build an idea of how individuals might rationalise their behaviour, thematic analysis was used. Unlike the behaviour of individuals, all six phases of the thematic analysis process by Braun and Clarke (2006) were employed to help discern the rationalisations that individuals might use.

In Phase 1, the interview transcripts were created; this was followed by Phase 2, which involved reading through these transcripts to generate codes related to the ideas and concepts that arose in participants' transcripts. Once the codes for the three versions of the website were generated, the final product of Phase 2 was generating a project map for each version of the website based on its respective codes. The project map is an NVivo visualisation that visually illustrates the link between files and codes or between codes in a project. These project maps were used as the input for Phase 3. This phase shifted the focus towards generating themes based on grouping the relevant codes in the project maps together. Using a printed version of the project map, the relevant codes that could be grouped under a common theme were circled. This process was used to filter the large volume of codes into smaller initial themes. These themes were then used to draw up the initial mind maps for each version of the website. Part of this process involved the inclusion of colour in the maps. A mind map node with a green outline represents something related to encouraging honesty; nodes with an orange outline represent something related to encouraging dishonesty; and the nodes with grey outlines represent themes that were relatively neutral if looked at in isolation. They did not push individuals towards honesty or dishonesty; in other words, the POST-LOG version is used as an example in this chapter, but a similar process was applied to the other two versions of the website.

In the case of the POST-LOG version, the project map with 36 codes was filtered down into 24 initial themes to form the initial thematic map for the POST-LOG thought

processes and rationalisations. An extract of this initial map is shown in Figure 6.6. A second version of the thematic map was generated; it excluded quotations from participant transcripts to make it easier to view and subsequently filter down the themes in later versions.

Due to the relatively high number of themes identified, the initial mind map(s) had to be refined several times during Phase 4. The goal was to refine the themes so that they were more distinct and to reduce the number of themes by enveloping them in a larger theme. As a result, refinement in a few cases entailed a simple rephrase. Tables 6.2, 6.3, and 6.4 illustrate the refining process of each step by indicating the original themes encapsulated in square brackets in the right-hand column and the new or refined themes in the left-hand column. The refinement process was carried out three times. A similar process was carried out for the Control and the PRE-LOG as well, with their respective maps and tables shown in Appendix D. Figures 6.7 to 6.10 illustrate this process for the POST-LOG version with regard to the rationalisations that were revealed after the analysis of the transcripts. It is worth noting that the mind maps for the three versions were not developed in isolation for each version. While working on the POST-LOG version, the other two versions' mind maps were also examined to help track any potential common themes that might emerge.



Figure 6.6: Initial thematic map POST-LOG thought process and rationalisations extract (Phase 3)

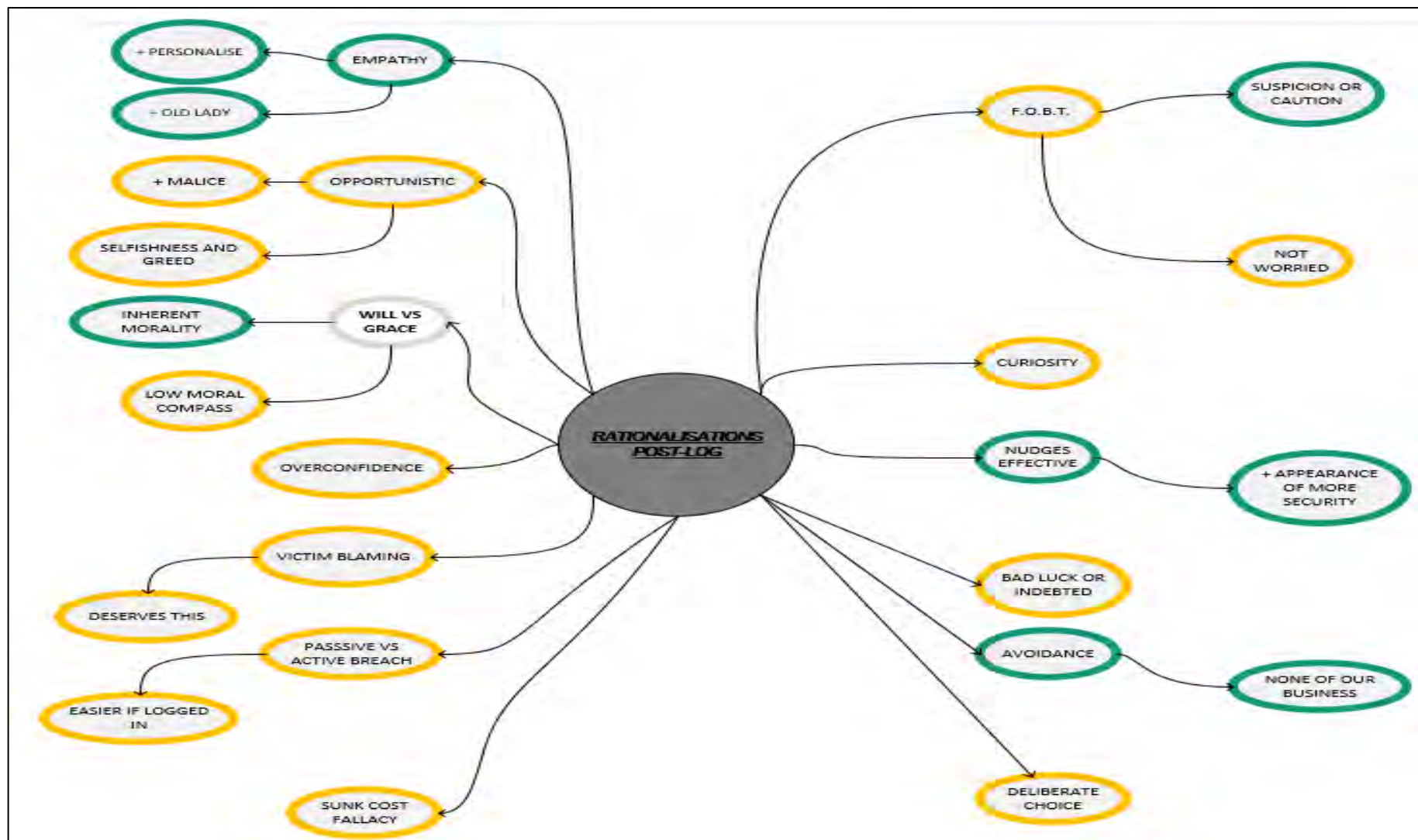


Figure 6.7: Initial thematic map POST-LOG thought process and rationalisations (no quotations version) (Phase 3)

Table 6.2: POST-LOG rationalisation refinement 1

| Refined theme(s) | [Original theme(s)] |
|---|---|
| Can better picture victim. | [Empathy] (+ child ideas) |
| Teach victim a hard lesson. | [Victim blaming], [deserves this], [malice] |
| I'm not so bad because I didn't actively compromise the account myself. | [Passive vs active breach] (+ child ideas) |
| Low or acceptable chances of detection. | [Overconfidence], [not worried] |
| Social norms – do not get involved. | [Avoidance] (+ child idea) |
| Opportunity to enrich self. | [Selfishness and greed] |
| Some people, by nature, are dishonest/honest. | [Inherent morality], [low moral compass] |
| Perception of higher chances of detection. | [Nudges effective] (+ child idea) |
| Opportunity and temptation + BIASED/FLAWED LOGIC. | [Curiosity], [sunk cost fallacy] |
| Opportunity legit? | [Suspicion or caution] |

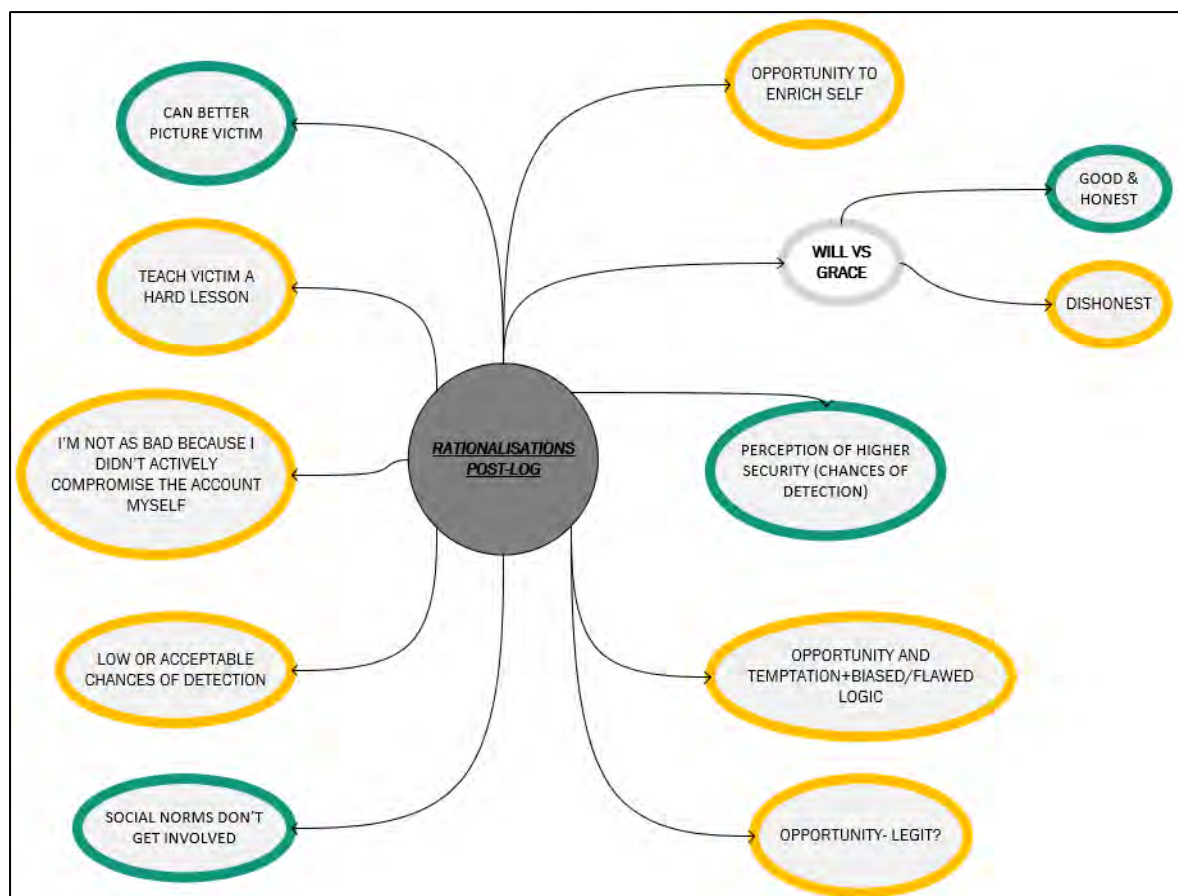


Figure 6.8: POST-LOG thought process and rationalisations refined V1 (Phase 4)

Table 6.3: POST-LOG rationalisation refinement 2

| Refined theme(s) | [Original theme(s)] |
|--|--|
| People's inherent nature dictates response to opportunity or scenario. | [Some people by nature are dishonest/honest], [opportunity to enrich self] |
| Harming real person is much harder. | [Can better picture victim] |
| Moral self-concept threat reduced. | [I'm not so bad because I didn't actively compromise the account myself] |
| Justify exploiting fraud based on biased logic. | [Opportunity and temptation + BIASED/FLAWED LOGIC], [opportunity legit?] |
| Hurt them because of their mistakes. | [Teach victim a hard lesson] |
| Perception of higher chances of detection. | [Low or acceptable chances of detection] + [perception of higher chances of detection] |

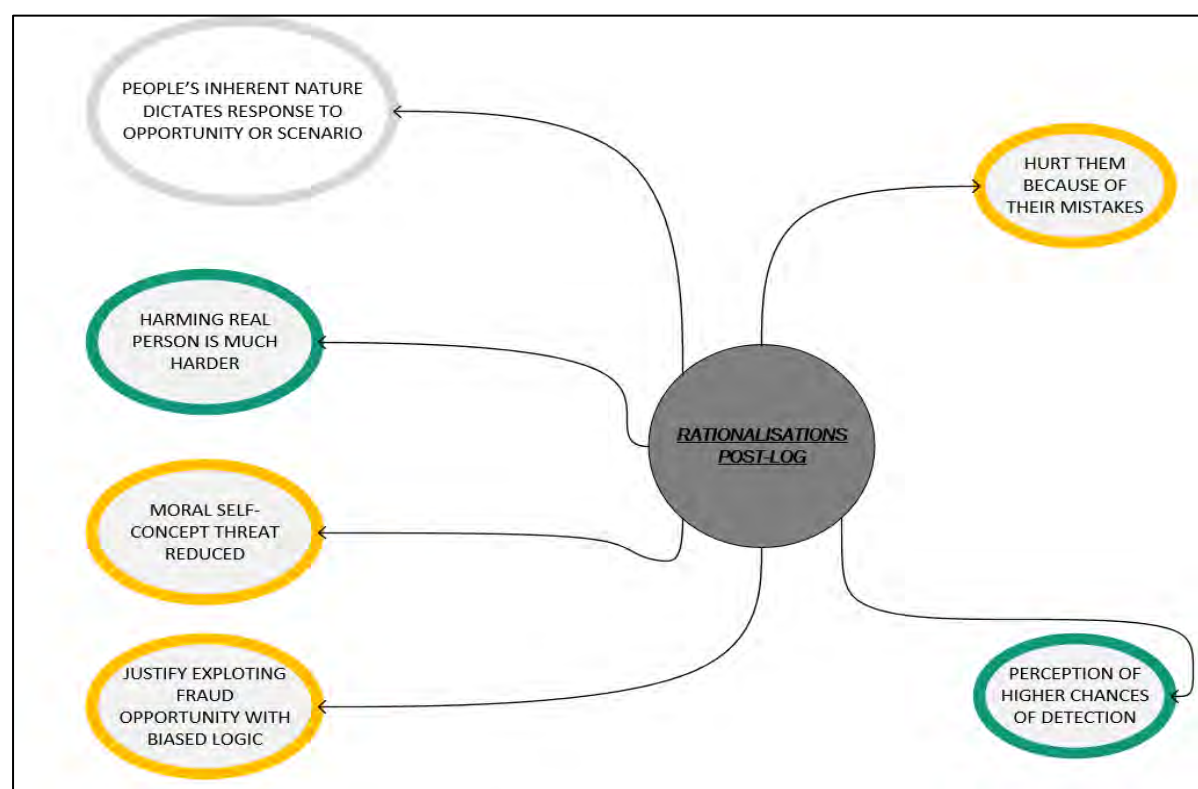


Figure 6.9: POST-LOG thought process and rationalisations refined V2 (Phase 4)

Table 6.4: POST-LOG rationalisation refinement 3

| Refined theme | [Original theme(s)] |
|---|--|
| Inherent nature and importance of self-concept. | [Harming real person is much harder], [moral self-concept threat reduced], [people's inherent nature dictates response to opportunity or scenario] |
| Justify fraud using biased or selfish logic. | [Moral self-concept threat reduced], [hurt them because of their mistakes] |
| Perception of higher chances of detection. | Perception of higher chances of detection |

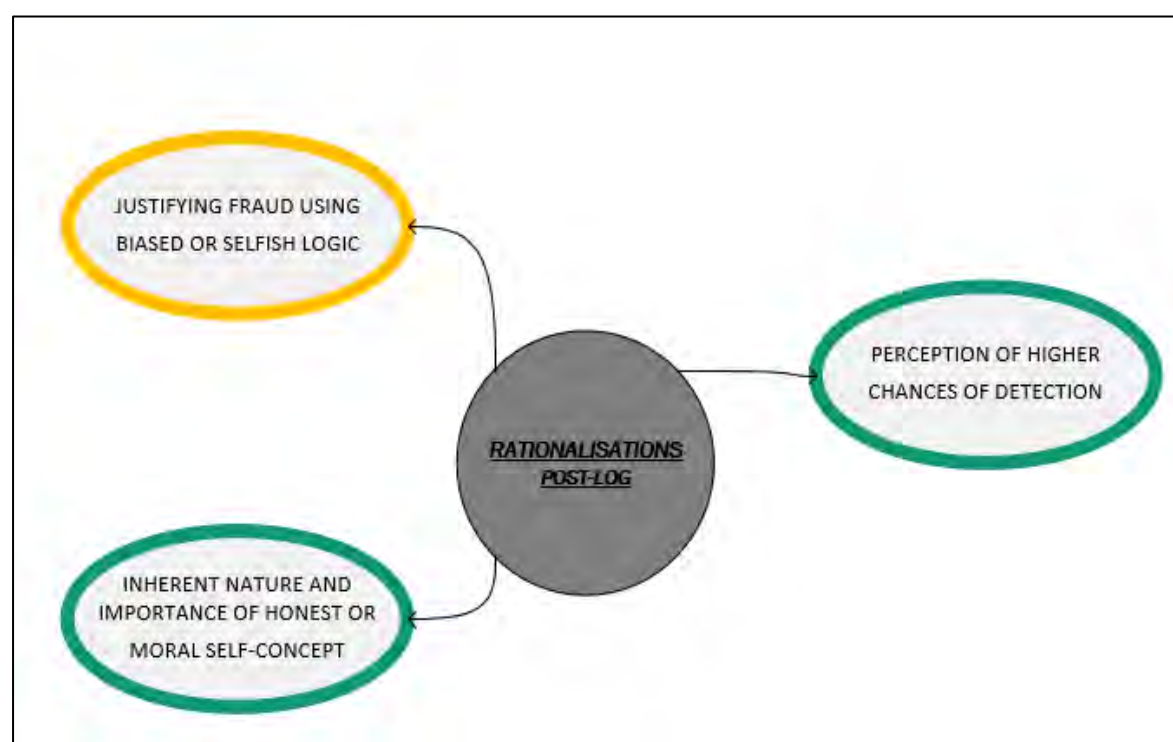


Figure 6.10: POST-LOG thought process and rationalisations refined V3 (Phase 4)

After all three versions of the mind maps were refined, the rationalisations were analysed once more, and combined into a single map that encompassed all the significant or unique rationalisation themes discovered in this study. This combined map represents all the rationalisations as the final product of Phase 4. This map is shown in Figure 6.11. This combined version had eight main themes and formed a synthesis of the different themes and ideas from all three versions. It is still not quite a candidate thematic map, as the eight main themes are the general rationalisations that the participants brought up during the interviews. This map was used as the input for Phase 5 of the thematic analysis process.

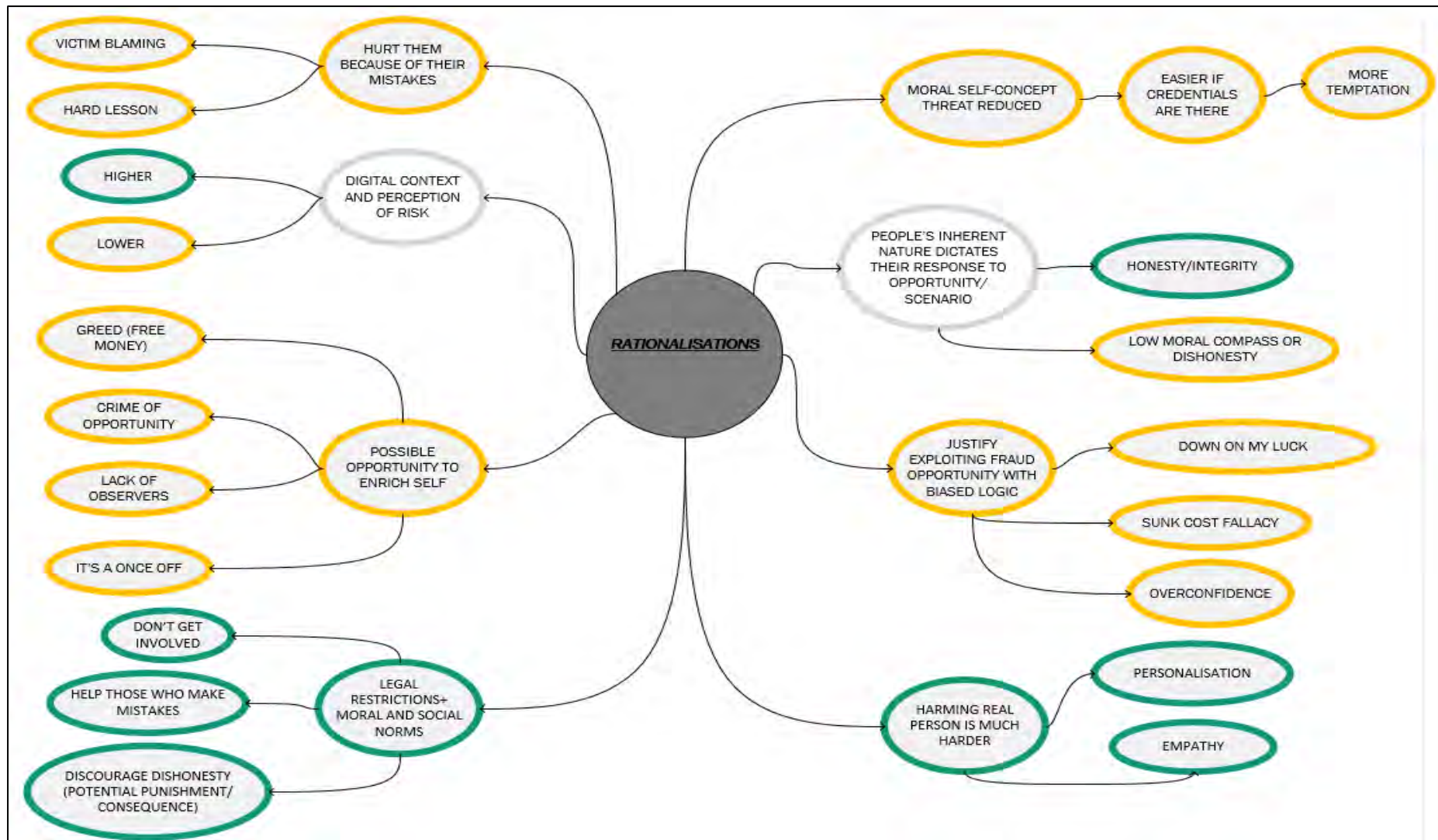


Figure 6.11: Rationalisations thematic map derived from all three versions (Phase 4 product)

6.5.1 Hurt Them Because of Their Mistakes

This unique rationalisation was initially difficult to categorise and compress into a larger theme, as it suggests that a third party may commit online banking fraud to punish the account holder. By defrauding the account holder, the third party effectively teaches them a lesson about the importance of keeping their account and credentials secure at all times. Once learned, the account holder would be very unlikely to repeat the error due to the financial damage done by the third party. Based on the context of online banking, this sense of “no room for mistakes” may have arisen due to the sensitive nature of dealing with individuals’ personal finances. As mentioned in Chapter 1, mistakes that leave credentials vulnerable may result in significant financial loss.

P11: “Hey, she’s got, you know, \$7700 here in her account. Maybe I could, you know, using her account number order something off Amazon or something like that, because you know, she... if she was gullible enough or stupid enough to leave without logging out, then she kind of deserves some kind of punishment for that, you know, and by that, meaning, you know, I can buy this \$500, whatever. And I’ve just found in my life that, like I said before, people tend to justify bad behaviour by saying well, you know, like victim blaming and, you know, but she kind of deserves this for, for leaving their account open in a public place like this.”

Participant 11 (Male, 63, Bachelor’s Degree)

P7: “I’ll teach them for being so stupid. I’ll teach them for being so stupid. There are a lot of reasons to...”

R: “That was pretty interesting. I’m sorry that that last one is kind of new. I’ll teach them for being...?”

P7: “Oh, I’ll teach them to be so careless. By taking advantage of their stupidity.”

Participant 7 (Female, 49, Bachelor’s Degree)

6.5.2 Digital Context and Perception of Risk

This was a very common theme in most interviews. The digital context requires additional steps and capability to exploit the opportunity, but it is still similar to other undeserved money experiments or scenarios. A third party has the opportunity to steal another person’s money and use it how they please (Zhong, Bohns and Gino, 2010; Shu and Gino, 2012; Rosenbaum et al., 2014; Holt, 2019). The difference in the digital context that most participants brought up or were aware of was the potential to be

tracked down. The fear of being tracked was one of the more common factors that many participants mentioned or implied.

P12: "Umm, just because I think they would fear getting caught with charges of misusing somebody else's bank account or something of that sort. Because they have to put their, their name in and their account information and to be able to, to get that money, so, it's not like somebody just left cash on the table with no cameras where they just pick it up and run with it, there's, there's tracking information that tracks back to them."

Participant 12 (Male, 33, Master's Degree)

P13: "Well, for one thing, Vanessa could see who got her money. And she could report Jill, you know, with the expectation of her being punished for online theft. I mean, it's going to be obvious; Vanessa can easily see who took her money."

R: "Okay, so, Jill or the average third party would be worried that they'd be tracked down, and it would pretty much be traced back to them if they try to transact at all?"

P13: "Exactly."

Participant 13 (Female, 61, Bachelor's Degree)

P2: "So, I think that would kind of a not make him want to, you know, use this account because everything is going to be monitored, it could be, you know, traced back to him..."

Participant 2 (Male, 31, Bachelor's Degree)

P5: "Because they would have had to send it to something that would directly link to them..."

Participant 5 (Male, 47, Bachelor's Degree)

Unfortunately, this potential risk would not always be sufficient to stop someone from transacting. The responses suggested that when the risk was believed to be low enough, they could still commit fraud.

P12: "I think some percentage of criminals do think about the possibility of getting caught, but just don't think they ever will..."

Participant 12 (Male, 33, Master's Degree)

P13: "Thinking that she could get away with it. That would be the main motivator. If she felt like the chances of being caught were slim, that would encourage you to go ahead and do a transaction..."

Participant 13 (Female, 61, Bachelor's Degree)

On the other hand, if the chances of detection were perceived to be higher, some responses suggested that this could dissuade a third party from trying to commit online banking fraud.

P1: "Hmm, I think, maybe like where it says that the, umm, updated transaction monitoring system for anti-fraud. Like she might be concerned with that. If you were to login. Maybe they'd find out that she might have something to do with that."

R: "So, Jill would be worried about being traced or detected?"

P1: "Yeah, I feel like they'd somehow find out like by tracing her."

R: "And that would affect her. That would also factor into a decision to close the web page or with that."

P1: "Yeah, that probably makes her not want to have any ties into that."

Participant 1 (Female, 32, Associate's Degree)

P2: "Yeah. So, on the one where it was saved. Uh, once I logged on, he would have seen, like, this message about, like, fraudulent activity and how all, you know, purchases are tracked. So, I think that would kind of not make him want to, you know, use this account because everything is going to be monitored; it could be, you know, traced back to him. So, I think the second one, it gives you more reason not to do it, versus the first one, which, you know, kind of locks you in, and then you just do what you want, but this one had more like checks and controls I feel like."

Participant 2 (Male, 31, Bachelor's Degree)

Overall, the chances of fraud detection in the digital context of online banking seemed to be a significant factor for third parties to consider.

6.5.3 Possible Opportunity to Enrich Self

The potential opportunity to gain a boost to their own finances was often sufficient enough motivation for some to commit online banking fraud. With the opportunity having "landed in their laps", they would take advantage to cover some of their own financial concerns.

R: "So why would some people actually try and transact and steal essentially?"

P14: "Well, there's money there, you know. I mean, people down on their luck – people with not so high of a moral compass. People, you know, opportunists. You know, whatever..."

R: "Okay, and then, like, with that 10%, would they have a similar thought process? What would essentially be the rationalisation that 10% that would essentially use the access?"

P14: "Free money."

R: *"So it's essentially an opportunity to enrich themselves."*

P14: *"Yeah."*

Participant 14 (Male, 45, Some College)

R: *"Okay. And then, essentially, they still, they have a need in terms of their car that they need to fix or some sort of financial need in the scenarios that they probably be the main reason why they start trying to take advantage."*

P10: *"Yeah, people don't generally think. Oh, I want to go steal some money today. It's generally spur of the moment, and if they need money, they're gonna do what they can to get it."*

Participant 10 (Female, 75, Associate's Degree)

The rarity of such an opportunity was potentially another factor that motivated people to act upon it; the idea being that running into online banking credentials, or an open account, is relatively rare for the average third party.

P9: *"Especially if it's an inexpensive car bill, I mean, they're never cheap. But you probably would think it's, you know, it's one, might as well, a one-off. I will never have an opportunity to, like, to do this again, probably. And so, he'll be like, well, I don't want to pay the mechanic, 'cause it's really expensive. I have this opportunity, and I'll probably never get a shot to like to do this again."*

Participant 9 (Male, 34, Some College)

The scenario design may have also factored into this as some participants mentioned that an average third party would check for, or at least be concerned about, other customers or staff who could witness them committing fraud. It is rare to have a lack of witnesses in a public venue like an Internet café. Part of the rare opportunity may have been due to the perceived time pressure.

P2: *"So they've probably, you know, see if you know anyone's around looking, um, you know, if there's any cameras. Since I think if I can remember, no one was around. He'd probably feel safe doing it. Since there was a computer there already and the credentials were already there, um, you know, I think he would feel like he would be safe in, you know, using this login information."*

R: *"Okay, so he'd feel safe that because he's alone, and chances are there's no one who's going to actually spot, and he'll be fine, essentially."*

P2: *"Right."*

Participant 2 (Male, 31, Bachelor's Degree)

P4: *"The thought process okay, so they would, if they really wanted to do it, they probably would look around the coffee shop, be, like, well who would, who would notice, if I slid over to that seat or slid the*

computer to me, and how much time do I have; is this person in the bathroom or talking to someone? And if they've done it before, then maybe they're really fast and efficient, and can quickly do it, and have no qualms about it, and be cool with it, and really not worry about it. If they were inexperienced and nervous, then they would fumble, and maybe take too long, and have to figure out the interface of this bank's website..."

Participant 4 (Female, 46, Master's Degree)

6.5.4 Legal Restrictions + Moral and Social Norms

The potential legal or social consequences of getting caught committing online banking fraud could encourage people to behave in a more honest manner.

P4: "Yeah, I wouldn't. I would hope the person would not take the bait and not be tempted to do that because it is illegal and unethical. I never would, I would feel, I would feel so free... I wouldn't want to, and I would feel totally freaked out about it."

Participant 4 (Female, 46, Master's Degree)

P15: "Going further, it would be cautioned or put off by the... the screens that are up the handcuffs. And the monitoring. I don't think it prevents them from going further, but I think for those who might just do it out of curiosity. That's a warning that they maybe shouldn't do that. A reminder of what norms everyone in society should do, that sort of thing. The 1% or less that I said might go further, like a... I would call it a 'road bump'. It's a caution, but it doesn't. There's nothing to prevent them from actually going further, people. They're gonna try and transfer some money. They're gonna go ahead and do it. But I think that's a small, all very, very, very small part of the population."

Participant 15 (Male, 54, Some Graduate Studies)

Two social norms arose from analysing the transcripts. The first had to do with helping those who have made mistakes.

P7: "... 25% I think maybe would just log her off just as a goodwill measure to protect her and make sure that nothing bad happens to her bank balance..."

Participant 7 (Female, 49, Bachelor's Degree)

P11: "The average thought process. I really can only do this for myself, but I would walk up and say somebody has made a horrible mistake, and I need to save this person from their own stupidity."

R: "Okay, so, yeah. Everyone says they see that the previous user made an error and would want to help them."

P11: "Yes."

Participant 11 (Male, 63, Bachelor's Degree)

Linked to this norm was the idea of the golden rule. People behave in a more honest or pro-social way in the hopes that another individual would do the same (Bennett, 1979). This also touched on an element of empathy.

P6: Well, for example, I'm speaking on my behalf too if I walk by and see the woman left her account open – the thought processes. Oh no, let me log out for her because I don't want her to, you know, lose her money and for somebody to go into her account. That's the thought process. I put myself in her place."

R: "Okay, so essentially empathise with Vanessa, that in this scenario."

P6: "Yes, and especially, she's a little bit older. So maybe she's not so techie. Maybe she just doesn't have a lot of experience with technology. Maybe she's just used to, you know, working from home. During her work from home and she, she just is not so aware that you have to log out. Maybe she just didn't even know, or maybe she forgot but no matter what, I would definitely log out for her."

Participant 6 (Female, 66, Bachelor's Degree)

P1: "Well, I personally wouldn't want someone to look into my information, and she might feel like it's best to log out."

Participant 1 (Female, 32, Associate's Degree)

The second had to do with not touching or taking other individuals' property without their permission.

P6: "Yes. I don't think I would even delete the username or password. You know I, you shouldn't really touch things that don't belong to you. So, I feel that just taking her device and giving it to the cashier or the customer service person should be enough to secure it."

Participant 6 (Female, 66, Bachelor's Degree)

P12: "75%, I think, yes, I would see somebody, you know, a bank account with somebody's login information that's not theirs and not touch that account. But well, knowing that there are consequences, but they don't want to deal with."

Participant 12 (Male, 33, Master's Degree)

To avoid the potential consequences of being labelled or even mislabelled a thief, some individuals may avoid touching or interfering with the account at all.

P6: "Because that's what I would want somebody to do for me. And it's not... I don't want to touch her, her device. I don't want to be accused of, you know, if I try to delete it. Later, is somebody going to come and say I tried to hack into her account."

Participant 6 (Female, 66, Bachelor's Degree)

P7: "I think that it may be, like, 25% would just do nothing and just leave it as is and, and not mess with it at all. Maybe because they're worried about being not caught, but, you know, just... I get I'm having trouble explaining it, they kind of like how people will see something bad going on and just not want to get involved. And so, I feel like 25% of the population may just be hands-off and just move to another computer or something like that."

Participant 7 (Female, 49, Bachelor's Degree)

6.5.5 Moral Self-Concept Threat

Generally, this theme refers to people who minimised any negative threat to their moral self-concept by rationalising their actions. In general, this meant they used circumstances or scenarios to reduce the negative impact on their self-concept from committing or considering committing online banking fraud. While unique, this rationalisation was only brought up by one participant, who suggested that in the POST-LOG scenario, not having to actively search for or steal credentials made it easier to justify succumbing to the temptation.

P2: "Yeah, and like I said, it was already logged in, I think he might feel like he's not really, you know, breaking into this person's account because it was already logged in to the account, but he would be less guilty compared to, like, the first scenario where you know he had actually log in. I kind of view it as, like, people who walk into a house with an open door. People do that as, like, all you know you're, if you break the door, you're committing a crime but just walking into a door that's open... you feel less guilty, I suppose. So, I think that's what he'll be feeling is, you know, since there's this computer is already logged on to the account, it's not really breaking and entering. You know, he says, you know, not as guilty. Yeah but, you know, from his point of view."

Participant 2 (Male, 31, Bachelor's Degree)

6.5.6 People's Inherent Nature Dictates Their Response to Opportunity/Scenario

Brought up by several participants was the issue of people's inherent nature. The responses suggested that some people are more honest than others by their inherent nature. Their nature then informs how they may react to the scenario where they may potentially be able to commit fraud. Those who were more honest by nature were significantly less likely to respond to the scenario opportunistically but instead would try to prevent others from abusing the vulnerable victim.

R: "Okay, now I'm gonna give you remote control, and you essentially play the role of, yeah, Jack, or the average third person visiting the website."

P8: *"Okay, so I'm an honest person, and I see someone who isn't me up on the screen, so I would go to 'if it isn't you, click here'. It's not doing anything, but that's where I would go. There we go."*

R: *"Okay, so the average person would log out... So why would pretty much the average person hit the 'If this isn't you, please click here'?"*

P8: *"Yes, well, because I think I and I think most people are relatively honest. I have no need to see this woman's banking information, and I certainly want it, wouldn't want to do anything that would cause her any harm. So, the first thing I would do is correct it and switch it to me."*

Participant 8 (Male, 65, Master's Degree)

R: *"Okay, and then just a quick one in the 35%. Why would they close up the browser?"*

P13: *"Um, I still want to believe that most people are honest that, that they wouldn't just steal something even if the opportunity is there."*

Participant 13 (Female, 61, Bachelor's Degree)

R: *"So now sharing, and then I'm going to give you remote control. Okay, so now, remote control, and you just role play whatever the average person would do on this website."*

P11: *"I'm only restricted to what I can do on the website. I can get really in a real-world situation. I would shout out and say, 'Hey, are you still here?' But barring that. [Logs out]."*

R: *"So, would the average third person also do something similar?"*

P11: *"I would like to believe that, yes."*

...

R: *"Yeah. There wasn't anyone else in the café."*

P11: *"If there was nobody else, that's what I would have done. And I think probably most people would also."*

Participant 11 (Male, 63, Bachelor's Degree)

Those who were by nature more dishonest tended to take advantage of the opportunity to defraud the vulnerable victim in the scenario. They were more concerned with how much they could gain rather than how much the victim would be hurt. Stopping them from exploiting such an opportunity would be more difficult.

R: *"Okay, and then would the rationalisation be similar to that 1%?"*

P15: *"Yeah, sorry, I think that, that I think when we get down to the 1% or less, you're talking about people that I think are not concerned by warnings. They're gonna do stuff anyway. It's more in their nature and their character to go as far as they can go. Yeah, I just think that group is a bit more hardcore in terms of what they'll do."*

Participant 15 (Male, 54, Some Graduate Studies)

R: “So why would some people actually try and transact and steal essentially?”

P14: “Well, there’s money there, you know. I mean, people down on their luck. People with not so high of a moral compass. People, you know, opportunists. You know, whatever. Better safe and [sic] sorry, you know...”

Participant 14 (Male, 45, Some College)

6.5.7 Justify Explaining Fraud Opportunity with Biased Logic

This theme generally looked at the use of biased or self-serving rationalisations that third parties may use to commit online banking fraud. There were three biased rationalisations that were hinted at in the participants’ responses. There was a little overlap with the “Possible opportunity to enrich self” theme.

The “Down on their luck” responses suggested that third parties may use a recent string of bad luck or financial setbacks to help rationalise committing online banking fraud.

P9: “Yeah, yeah, because you probably would just think, well, it’s expensive for a mechanic. And I have the opportunity. Umm, and I really don’t want to pay this expensive mechanic bill. If I’m gonna do it...”

Participant 9 (Male, 34, Some College)

R: “So why would some people actually try and transact and steal essentially?”

P14: “Well, there’s money there, you know. I mean people down on their luck...”

Participant 14 (Male, 45, Some College)

The “sunk cost fallacy” responses generally looked at the idea that by having explored someone’s account so much, an individual might as well go further and commit online banking fraud, despite the known risks. Individuals are aware that they know they have done something wrong by already being in the account.

P10: “Hey, probably would have had second thoughts. It looks like somebody’s going to be able to track me and tag me, and maybe I shouldn’t have done this. But I’m this far, so I might as well, and they did.”

R: “So almost like sunk cost, in that they’ve already gone so far, they’re just gonna go proceed?”

P10: “Yeah, like if you jump in the water. It’s cold doesn’t make any difference. You’re already in the water ...”

Participant 10 (Female, 75, Associate’s Degree)

Unlike Participant 10, some responses suggested that not all individuals would explore the account but not commit an unauthorised transaction.

R: "Okay, so if they're logged in, what do they also try and transact, or would they just log out?"

P7: "I think it's a mix. I know there is probably a decent percentage of the population that would see what they could get out of it, you know, and conduct a transaction. But, and I'm trying to think of what I feel like, maybe 30% of the average population would try to conduct a transaction and, you know, buy something with her balance. But I'd like to think that, you know, 70% of the population would just be looking just out of curiosity, but not really doing any harm to her. Think about, excuse me, her bank account balance."

Participant 7 (Female, 49, Bachelor's Degree)

Underlying both extracts from Participants 10 and 7 is the idea that third parties may be curious and explore the account. Throughout this exploration, there is temptation, but not all may succumb.

P1: "I think it might take a little time just to actually understand what she's looking at, and maybe there's a little curiosity, this looks around, but then she'd just want to log out, realising that it's probably not the best thing to do."

Participant 1 (Female, 32, Associate's Degree)

P15: "I think some people are just naturally curious, and they're going to check it out a little bit. Further, you know I, when I saw \$7 000 in the bank account, I thought, well, that would be nice for me to have. But out of curiosity, I'm certainly not going to transfer the money into my account ..."

Participant 15 (Male, 54, Some Graduate Studies)

The "overconfidence" theme generally focused on the idea that individuals, despite being aware of the risk, were still confident that they could commit fraud without being tracked down. Regardless of how (in)accurate their perceived low chances of detection were, they believed they could "beat the system".

P12: "Think some percentage of criminals do think about the possibility of getting caught, but just don't think they ever will."

Participant 12 (Male, 33, Master's Degree)

R: "OK, and then... So, looking back on the last question. Uh, looking back at all three versions. What might have had the... what might have had the most potent effect on, like, Jill or average third party's behaviour? What aspect of the interfaces?"

P13: "Thinking that she could get away with it. That would be the main motivator. If she felt like the chances of being called were slim, that would encourage you to go ahead and do a transaction."

Participant 13 (Female, 61, Bachelor's Degree)

R: "Okay, so essentially, the average person or random third party would probably transact and try and make a payment, right?"

P10: "Yeah, even though they're being traced, people seem to think they can beat the system."

Participant 10 (Female, 75, Associate's Degree)

6.5.8 Harming a Real Person Is Much Harder

Most banking interfaces only have a name and account information, which makes it very impersonal. By including a face, people can associate the account with a name, and an account number made it more apparent that the victim was a "real" person. In simpler terms, it made empathising with the victim much easier and subsequently made committing fraud more difficult for most. The POST-LOG was the only version where such a nudge had been employed.

R: "Huh, okay, umm. So just gonna do a quick one. So, looking back at, well, thinking back to the previous page, was there, would anything have stood out to Jill?"

P1: "Umm, I think, like, the person's name and the image of the woman. Like, she might think, like maybe that's the woman, there like it. It kind of, like, personalises it a little more. So that might make her feel, like, guilty for, like, looking through someone's things."

Participant 1 (Female, 32, Associate's Degree)

P3: "So I think that seeing the picture here makes it, like, very personal, and I think that this person in the scenario would feel very bad about, like, tampering with any information here. With this, with two large pictures staring at you and she's obviously an older woman. She's smiling. She seems friendly, so I would probably log out in this case or hit 'If this isn't you, click here', so I'd probably do the same thing. I mean, do the right thing here. Hit click here."

Participant 3 (Female, 30, Bachelor's Degree)

It was relatively common for the participants to reference this nudge as a major factor in dissuading dishonesty. Part of this effect, it seems, could be attributed to the choice of account holder in the scenario, i.e., having a "sweet old lady" there helped, sometimes, by getting people to think of their elderly friends or relatives.

P7: "I would immediately, I would see the picture, and I would probably think about my parents and think if they, if something like this happened to them, I wouldn't want someone to take advantage of them. So, I would go ahead and just click the logout button to get them to remove the connection to her account so that nobody could come back and take funds from her. Now with the average person. I feel like, you know, like I said, 25% I think would do like what Jill did. You know, have someone in mind that you think I wouldn't want my loved one to have to go through this. So, let me log her out and just do her a favour."

Participant 7 (Female, 49, Bachelor's Degree)

There were a few cases where personalisation backfired, i.e., having an older account holder was a factor that tempted rather than dissuaded individuals from committing online banking fraud.

R: "Okay, I'm going to give you remote control, and you can just role play what Jill or the average third party would do."

P13: "Okay. This one would be much for tempting for Jill to put in her name and account information, so she could steal money from Vanessa 'cause Vanessa looks elderly. At first glance, you wouldn't think that Vanessa would have real good control of her finances. Although her transaction history looks sparse. Jill, if Jill really felt desperate for money, she probably would try and slip in a transaction and count on Vanessa not noticing due to her age."

Participant 13 (Female, 61, Bachelor's Degree)

R: "Okay. So, okay. So, to criminal Jack, what stood out was the name. The account number and the picture, what else?"

P5: "Picture. And that she's a bit older. So, she'd be less likely to catch on to what's happening."

Participant 5 (Male, 47, Bachelor's)

The rationalisation-related themes discussed were compressed into three final main themes and four subthemes. These themes are illustrated in the thematic map in Figure 6.12. This final thematic map for the rationalisations, along with the descriptions of the themes, represents the product of the fifth phase of thematic analysis.

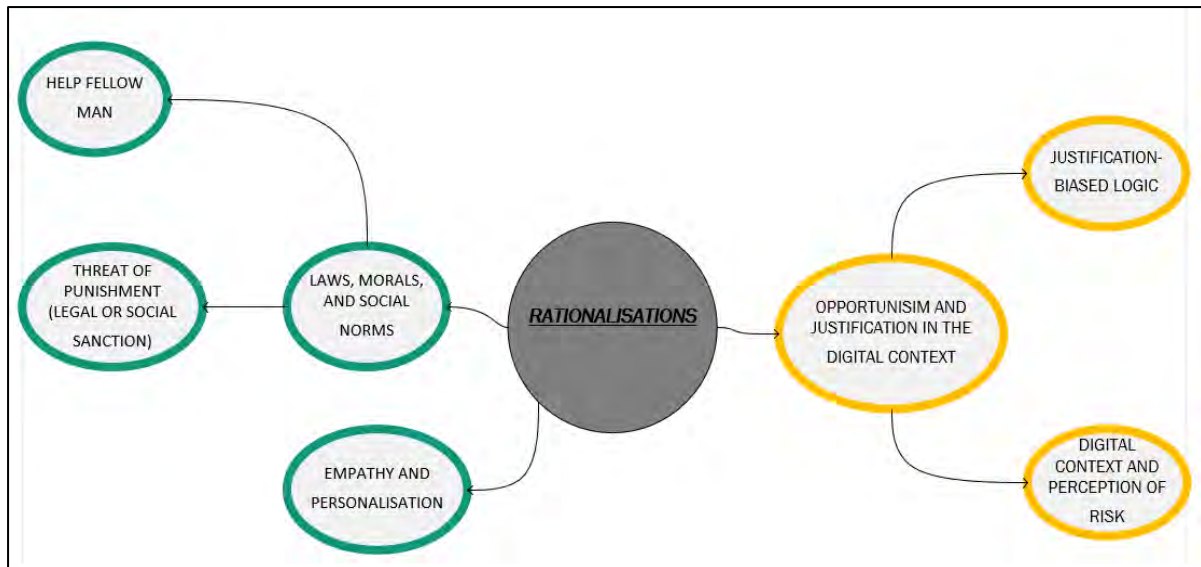


Figure 6.12: Rationalisations final thematic map (Phase 5 product)

6.5.9 Opportunism and Justification in the Digital Context

This theme encompasses individuals' behaviour in the digital context of online banking when presented with the opportunity to potentially commit fraud. Online banking inherently comes with the risk of being tracked or observed, as there are logs or digital "breadcrumbs" that may reveal details about transactions done and who was involved. With the risk of being tracked present, online banking carries a greater risk of being caught committing online banking fraud. This risk is often a consideration made by individuals in scenarios where they have the opportunity to commit online banking fraud. Anything that reduces the perceived risk is generally fraud-enabling, while, on the other hand, anything that raises perceived risk is often fraud-discouraging.

When individuals are tempted to or decide to commit online banking fraud, it is usually due to the use of some biased or self-serving logic. This logic allows them to justify behaving in a way that benefits themselves despite knowing that committing fraud is dishonest. The fraud-enabling rationalisations (orange-coloured themes and subthemes from Figure 6.12) were grouped under the subtheme "Justification-biased logic".

These rationalisations included the following:

- Down on their luck;
- Lack of observers in the area;
- Greed;
- Sunk cost fallacy and curiosity;
- Overconfidence and lower perceived risk of detection;
- Inherent dishonest nature;
- Accessing an open account is not that bad (moral self-concept maintenance);
- Crime of opportunity; and
- Hurt them because of their mistakes.

6.5.10 Empathy and Personalisation

When some form of personalisation is added to an online banking interface/website, it becomes easier to empathise with the person behind an online account. This, in turn, can make it more difficult for someone in such a scenario as described in the experiment to commit online banking fraud. Personalisation may not always have a desirable effect, as different account holders may be perceived as more vulnerable than others. In other words, there is a slight chance it might be fraud-enabling, depending on the account holder.

6.5.11 Laws and Social Norms

As the name implies, this theme focuses on rules that guide behaviour. These rules may be enforced to varying degrees, but they still inform individuals' decisions and behaviour. These rules are generally fraud-discouraging. The first subtheme, "Help fellow man", focuses primarily on the social norm that encourages individuals to help others when they have stumbled or made a mistake. The participants mentioned how they or the average third party may attempt to prevent any further unauthorised mistakes because they recognised that the account holder inadvertently left their account vulnerable, which is possibly carried out by individuals who are more inherently honest.

The second subtheme, "Threat of punishment", looks at the rules that govern how one may interact with the property of others. These rules promise some undesirable

consequences for being caught stealing or perceived as being a thief, i.e., using another person's property without permission. Legally, these consequences may come in the form of criminal prosecution, or social consequences in the form of a damaged reputation or ostracisation. People are so afraid of such consequences that they may avoid contact with the computer or online banking account to avoid being labelled or even mislabelled as a thief.

6.6 Summary

This chapter explained the findings from analysing the primary data collected for this study. The first subsection of this chapter examined the sample (n=15) from which data were collected. While there were slightly more male than female participants, all the age strata were balanced with five members each. In terms of education, all participants had reached a tertiary education level, with the vast majority holding bachelor's degrees.

In terms of behaviour, the vast majority of participants' responses suggested that the majority of third parties in similar circumstances would be "honest" and would not transact. It is worth noting that the PRE-LOG version still had an "honest" majority; it was very close to being an even split. Overall, the responses suggested that the POST-LOG version was likely to be more effective in influencing the behaviour of third parties. While a significant portion suggested that combining the PRE-LOG and POST-LOG versions would be beneficial, the majority believed it would have no additional effect.

Questions were included in the interview to help identify which choice architecture manipulations were noticed and may have affected behaviour significantly. In the PRE-LOG version, the most significant aspects were the "Updated TMS" messages, the image of handcuffs, and the "big eye". For the POST-LOG version, the most significant aspects were the image(s) of Vanessa, the account holder, and the "If this isn't you, please click here" option. Overall, the image of Vanessa was the nudge that the participants noticed.

Approximately nine rationalisation themes that could encourage or excuse committing online banking fraud emerged. They were grouped under the theme "Opportunism and justification in the digital context" and its subthemes. In terms of reasoning or

rationalisation to discourage dishonesty, there were two themes: “Laws, morals, and social norms” and “Empathy and personalisation”.

The subsequent chapter examines the potential implications of these findings for practice and theory.

CHAPTER 7: DISCUSSION

7.1 Introduction

The previous chapter presented the research findings discovered from analysing the primary data collected for the study. This chapter seeks to discuss those findings further, and link them back to help answer the research questions originally proposed in Section 1.4. Sections 7.2, 7.3, and 7.4 each focuses on discussing and answering one of the research questions. This chapter also presents the final phase of the thematic analysis process as outlined by Braun and Clarke (2006).

7.2 Goals of the Research Revisited

The study had three goals. Firstly, to investigate how effective various nudges were in making it difficult for someone to rationalise committing online banking fraud, and subsequently reveal which nudges would be best able to dissuade instances of online banking fraud. The second goal was focused on where it is ideal to deploy nudges to give the best chance of dissuading online banking fraud. The final goal was to explore and discover some of the rationalisations individuals may use to commit online banking fraud.

7.3 Effective Nudges

This section discusses the effectiveness of the nudges employed on the websites to dissuade online banking fraud. It provides an additional discussion of the findings in Section 6.3. This discussion section aligns with the first research question:

RQ1: Which choice architecture manipulations (“nudges”) are the most effective at dissuading online banking fraud?

As mentioned in Section 5.5.3, the Control version served as the base website, which was modified and tweaked to create two alternate versions, the PRE-LOG and the POST-LOG versions. These versions and the various nudges (choice architecture manipulations) employed can be found in Appendix B. Ignoring the effect that each

individual nudge may have had, one of the reasons the findings may have revealed the POST-LOG version to be more effective was the number of nudges employed. The POST-LOG version employed approximately 17 nudges, compared to the PRE-LOG version, with approximately eight nudges. This may have affected the comparison between the two versions. “Approximately” is used here because some nudges incorporated multiple choice architecture manipulations. This difference was brought up in interviews as a participant mentioned that the POST-LOG version had an element of repetitiveness.

P12: “It’s hard to pick just one, but the overall repetitiveness. The fact that there is something every step, literally, from the time I saw you know the screen of. ‘Here’s the photo. Is this you?’ I’m having that repetitiveness, or I have to be faced with it. Oh, I’m committing a crime, or they know they’re going to catch me...”

Participant 12 (Male, 33, Master’s Degree)

In terms of the imbalance in the number of nudges, this occurred because, as envisioned/assumed when devising the choice architecture of the website(s), there are more opportunities to nudge a third party to not commit fraud. Assuming an individual does not have access to another person’s online banking account, fundamentally, there is much less available functionality on the website, which subsequently gives a third party little to no opportunity to commit online banking fraud on a website. Whilst Chapter 4 hinted at several nudge mechanisms, employing them in the specific context of online banking was a challenge. This can be seen in Appendix A, as not all the provided examples were in an online banking context. In other words, although they were many nudges, not all would translate to the context of trying to prevent a third party from committing online banking fraud. The original context of Jesse and Jannach (2021) was the potential nudge mechanisms that could be employed to improve digital recommender systems (e.g. e-commerce, user and product reviews, or recommendations). The focus of designing the PRE-LOG version was what an average user would encounter if they wished to access their bank account online and what could be changed to help prevent online fraud, given the limited functionality available.

Moving beyond the number of nudges in each version, some were deemed more effective than others. As mentioned in Section 6.3, the most effective nudges in the PRE-LOG version were the messages regarding the “Updated TMS”, the handcuffs

and associated fraud scheme message, and finally, the “big eye” that was prominent on the page. All three of these nudges on the PRE-LOG version generally focused on discouraging online banking fraud by signalling to third parties that the website is more secure because transactions and accounts are carefully monitored. This is also linked to the rationalisations regarding tracking risk within the digital context.

The Updated TMS messages employed nudge mechanisms such as the spotlight effect, salience, and order effects (Acquisti et al., 2017; Caraban et al., 2019; Jesse and Jannach, 2021). These nudges aimed to make rationalising committing online banking fraud difficult by targeting specific (sub)factors within the COM-B model (see Section 3.2). In this case, psychological capability and reflective motivation applied. These nudges were meant to bring to the forefront of an individual’s thoughts the idea that the transactions on the site were very carefully monitored and subsequently made a third party reconsider their actions or consider being caught.

The handcuffs employed the nudge mechanisms of warning, salience, and priming in terms of influencing rationalisations. These nudges targeted psychological capability, except for the priming aspect, which targeted both reflective and automatic motivation. The nudges were intended to give unauthorised third parties pause by invoking the image or idea of being caught and punished for committing a crime. This image or idea would then ideally stay in their mind as they continue to use the website.

The “big eye” worked in conjunction with the Updated TMS message as it was placed next to the message on the website. It employed nudge mechanisms such as spotlight, salience, and order effects. The target for this nudge was an individual’s psychological capability and automatic motivation. The prominent eye draws an individual’s attention, and then they, ideally, read the Updated TMS message placed next to it. This is ideally due to its prominence and the symbolic association of the eye with surveillance (Koskela, 2000; Wilson, 2020). The idea that their actions were being observed or recorded would be placed at the back of their mind. The Updated TMS message was rated the most effective of the three PRE-LOG nudges.

On the POST-LOG version, the most effective nudges were Vanessa’s image(s) and the “If this isn’t you, please click here” link. Both nudges focused primarily on the mechanism of instigating empathy, by getting a third party to “picture” and imagine the impact of fraud on the third party. As a result, they focused on social opportunity and

reflective motivation factors. Section 7.5 examines the rationalisation aspect in more detail. As mentioned earlier, the POST-LOG version of the website was considered more effective in discouraging third parties from committing online banking fraud. Unsurprisingly, the most effective nudge in this version, the image of the account holder, Vanessa, was considered, overall, the most effective nudge to dissuade online banking fraud.

Overall, from the nudges employed, personalisation and creating a stronger impression of website security and monitoring seem to be the most effective ways to dissuade individuals from committing online banking fraud. Among these two paths, employing personalisation was the more effective. The next section discusses where these nudges could be deployed on an online banking interface to give them the best chance of dissuading online banking fraud.

7.4 Deployment of Nudges

This section of the discussion switches the focus to the findings related to the likely behaviour of third parties for each version of the website and its respective scenario. This will help to gain a sense of which version of the website was the more effective in terms of dissuading individuals from committing online banking fraud. This section is therefore aligned with the second research question:

RQ2: When comparing the placement of nudges before and after logging in, where is it more effective to deploy nudging to dissuade online banking fraud?

The participant responses generally suggested that third parties who found themselves in similar scenarios as the ones devised for this study were more likely to behave honestly. In other words, they were likely to not abuse their access to another individual's credentials or account to commit online banking fraud. This overall pattern, if viewed in isolation, would be encouraging, as it would suggest that most people are not going to use a similar opportunity to commit online banking fraud. This pattern provides some support for the "Grace hypothesis", i.e., people being inherently honest and needing to be tempted or convinced to act dishonestly (Amigud and Lancaster, 2019; Speer et al., 2020). However, if we focus on the specific versions of the website, some interesting insights emerge, i.e., the Control, PRE-LOG, and POST-LOG versions of the fictional Horizon Bank's online banking website.

For the Control version of the website, the broader trend for honesty was most prominent, as it had the largest majority of participant responses classified as honest. Of the 15 participants in the sample, 10 were classified as honest. However, this is odd, given that the Control version itself was designed to have no nudges in place to encourage honesty. When building the three versions of the website, the expectation was that the Control version would have the highest incidence of responses classified as “Transact”, which means that the participants’ response suggested that the third party in a similar scenario was more likely to perform unauthorised transactions, i.e., commit online banking fraud. Subsequently, the other versions, which included nudges, were then expected to deviate from this “baseline”, i.e., have fewer responses classified as “Transact”. With the data analysis revealing the opposite trend (baseline of “Honesty”), it does make it harder to evaluate any positive effect that employing nudging may have had on encouraging more honest behaviour in third parties. One possible reason the expected trend never arose was the difference in scenarios and choice architecture manipulations employed in the three versions. Where a traditional experiment alters one variable and keeps the others constant to help evaluate the effect that changing that specific variable has on the results, this did not translate perfectly to this study. The choice architecture in this context was the UI of an online banking website. As mentioned in Section 5.5.3, the Control version was the base version of the website for Horizon Banking, but the PRE-LOG and POST-LOG versions modified different aspects of the website by implementing nudges. The other “half” of the website for the PRE-LOG and POST-LOG versions, if visited normally, was the same as the Control, i.e., after logging in on the PRE-LOG version and before logging in on the POST-LOG version, the choice architecture was the same as the Control version. Overall, while the study may have attempted to keep the “other variables” constant, the instrument design and scenarios may have created versions that were effectively more different than anticipated, which inadvertently created scenarios where committing online banking fraud may have been more tempting. As long as this is kept in mind, comparing the three versions to gauge the effectiveness of nudging could still be useful, even if it is not a perfect “apples to apples” comparison.

All three versions of the online banking website generally trended to the “Honest” classification; however, the PRE-LOG version was by far the closest to an even split, with seven out of 15 responses being classified as “Transact”. As mentioned in

Chapter 6, while it was not the most noticed aspect of the choice architecture in this version, a significant number of participants suggested the credentials themselves as one of the things they noticed and focused on. If counted as choice architecture manipulation, it would have been ranked second on the PRE-LOG version in Section 6.4.1. Again, this goes back to the effect of the scenario and choice architecture design. If the credentials were not in the input fields, the findings might have been different, but the PRE-LOG was the version where a third party was anticipated to be the most likely to commit online banking fraud.

While the POST-LOG version had a better rate of “Honest” responses than the PRE-LOG version (9/15 as compared to 8/15), it still was not as high as the baseline set in the Control version (see Figure 6.4 in Section 6.4.1). Thus, even when factoring in the potential effect that the scenario and choice architecture design may have had on lowering the chances of a third party behaving honestly, the POST-LOG version of the website was more effective than the PRE-LOG version. This was also reflected in participants’ responses when asked which version of the website was more effective. As illustrated by Figure 6.5 in Section 6.4.2, most participants responded that the POST-LOG version of the website was more effective at dissuading online banking fraud. The implication here is that employing nudges on the interface after an individual has logged in to an online banking account is more effective than before they log in, which thus helps to answer the second research question:

RQ2: When comparing the placement of nudges before and after logging in, where is it more effective to deploy nudging to dissuade online banking fraud?

Regarding this research question, it is also worth noting that most participants’ responses suggested that combining both the PRE-LOG and POST-LOG versions would have a little additional effect on the behaviour of third parties on the website. In other words, the suggestion was that nudging individuals before and after logging in to an account would yield little additional benefit in discouraging online banking fraud. Nudging individuals after they have logged in may therefore be an ideal focus when implementing nudges on online banking websites. When seeking to understand why this finding may have arisen, it is helpful to look at the choice architecture manipulations employed on the website(s). Tables B1 and B2 in Appendix B specify which nudges were employed in each version.

7.5 Rationalisations

In Section 6.5, a candidate thematic map was generated that incorporated various themes discovered regarding participant rationalisation. This thematic map was then refined to help produce a final mind map (see Figure 6.12 in Section 6.5), which contained three main themes and four subthemes. Among these three main themes, “Laws, morals and social norms” and “Empathy and personalisation” generally dealt with encouraging honesty. The final main theme, “Opportunism and justification in the digital context”, encompassed factors that an individual may use to justify or excuse committing online banking fraud. Overall, all these themes aligned with the third research question:

RQ3: If a third party impersonates or defrauds the legitimate account holder, how do these individuals rationalise their dishonest actions?

However, the most direct answer to the research question comes from Section 7.5.3, as this subsection focuses specifically on the rationalisations that enable fraudulent behaviour to occur (to be justified).

7.5.1 Laws, Morals, and Social Norms

This main theme focuses on the various rules that guide the behaviour of people within society, whether they are laws or simply social norms. These rules may be enforced to various degrees, but they inform the behaviour of individuals in ways that generally dissuade them from committing online banking fraud. This main theme was split into two subthemes: “Help fellow man” and “Threat of punishment”.

7.5.1.1 Help Fellow Man

The first subtheme, “Help fellow man”, dealt with social norms that encourage more honest behaviour without necessarily threatening some form of sanction or punishment. As the name of the theme implies, the social norms encouraged helping others when they have made mistakes; in this context, recognising that the original account holder had made an error that left their account vulnerable and subsequently helping to prevent unauthorised access by other less honest individuals. Examples of the behaviour motivated by this norm include closing the browser window, alerting the

management of the Internet café, tearing up or disposing of the sticky note, logging out immediately, and clearing out the credentials field.

In general, this subtheme suggested that there may be individuals who are more inherently honest who would actively try to help other people in need. Part of this behaviour could be linked to the idea of the “golden rule” as people partially empathised or imagined what it would be like to be the account holder in the scenario (Vogel, 2004). Bennett (1979) suggests that this may be a relatively well-known norm in the USA.

As briefly mentioned, part of this theme involved helping prevent unauthorised access by more dishonest individuals. One participant explicitly brought up the idea that if the computer and credentials were left as is, someone would commit fraud eventually.

R: “Okay, so well, you’ve mentioned two versions, so just the first part? How likely do you think someone would be to actually hit the login button?”

P14: “I think it would be inevitable sooner or later.”

R: “Okay, so if you had to put like a percentage on the chances, what would it be roughly?”

P14: “Umm, like 90%.”

Participant 14 (Male, 45, Some College)

This suggested that those individuals who are more inherently honest would decide to help are in the minority. In terms of the “Will and Grace hypothesis” mentioned by Amigud and Lancaster (2019) and Speer et al. (2020), this lends credence to the “Will hypothesis” side of the spectrum. Based on the interviews, people tend to be more inherently dishonest and need to be nudged to behave more honestly.

The final norm under this subtheme was the idea that people should not touch or tamper with the possessions of others, which refers to the “respect for property” principle in Scott and Jehn’s (2003) conceptualisation of dishonesty. In essence, this social rule encourages people not to steal and can also help prevent online banking fraud.

7.5.1.2 Threat of Punishment

While still touching on social norms in terms of encouraging more honest behaviour, the second subtheme looks at the idea of how the potential punishment for being

caught stealing dissuades an individual from committing online banking fraud. The consequences or punishment, in this case, can arise from the legal or social sides. The former deals with criminal prosecution in a legal system, and the latter deals with social consequences. In both cases, the threat of an appropriate sanction or punishment for stealing encourages more honest behaviour, which subsequently provides support for the deterrence theory (Mehlkop and Graeff, 2010; Piquero et al., 2011; Tomlinson, 2016). Given the deterrence theory's roots in criminology, this is more applicable to the legal side, as individuals face potential criminal prosecution if caught committing fraud (Mehlkop and Graeff, 2010). The potential punishment if caught committing online banking fraud is a factor that most third parties in similar scenarios would consider.

When looking at the social side, being caught committing fraud can negatively impact the individual's social reputation or, worst-case scenario, their peer group ostracises them (Buonanno, Pasini and Vanin, 2012; Cartwright, 2019). The threat of being labelled a thief by others, even accidentally, could be a strong enough motivator for some individuals to avoid getting involved in the scenario at all. The potential damage to their social reputation could encourage individuals to behave more honestly. This partially aligns with the guilt aversion hypothesis brought up in other studies (Battigall and Dufwenberg, 2007; Khalmetski, 2016; Speer et al., 2020). People alter their behaviour to be more in line with what they believe others expect of them, but the insights that emerged seemed closer to what is suggested by the deterrence theory. Similar to legal prosecution, the avoidance behaviour implied an element of dread rather than guilt or stress that motivates individuals' behaviours in similar scenarios. Overall, when looking at the threat of punishment, the legal and social aspects can help prevent individuals from committing online banking fraud.

7.5.2 Empathy and Personalisation

As mentioned earlier, Vanessa's image in the POST-LOG version was the most effective nudge. This nudge focused on personalising the online banking account to trigger empathy. Based on the participants' responses, it had the intended effect for the most part. By personalising an online banking website's otherwise very concise and impersonal interface, it ideally becomes more difficult to steal from the account, as the victim or account holder can be more easily visualised. This will likely make a

third party reluctant to consider stealing from the account holder. One participant explicitly mentioned this:

P3: "So I think that seeing the picture here makes it, like, very personal, and I think that this person in the scenario would feel very bad about, like, tampering with any information here. With this, with two large pictures staring at you and she's obviously an older woman. She's smiling. She seems friendly, so I would probably log out in this case or hit 'If this isn't you, click here', so I probably do the same thing. I mean, do the right thing here in here. Hit click here."

Participant 3 (Female, 30, Bachelor's Degree)

Vanessa's image is placed in two places and is visible in the header of most POST-LOG pages. The "If this isn't you, please click here" link is next to the header's image. While the link targeted similar COM-B factors to Vanessa's image (social opportunity and reflective motivation), it also targeted psychological capability as it provided an additional option to allow a third party to back out and not commit online banking fraud. Also, by being almost ever present, the image and link serve as a constant reminder that this is someone else's account. Among these two, Vanessa's image was singled out as the most impactful aspect of the POST-LOG version. This suggests that adding more personalisation to online bank accounts and their interfaces on similar websites could be helpful in discouraging fraudulent behaviour.

A similar finding was reported by Holt (2019); except, in that case, it was the inclusion of a physical picture within a "misplaced" wallet rather than on an online bank account. Cohn et al. (2019) found that by including an item, in their case a key, that an individual can imagine would be valuable to the original owner, a "misplaced" wallet was more likely to be returned, which suggests that empathy with a victim may be a powerful motivator to encourage honesty. Ariely (2012) and Köbis et al. (2019) made a similar finding regarding discouraging dishonesty when they completed their undeserved money experiments.

Regarding personalisation employed as a nudge, a few points from Chapter 6 are worth reiterating. Part of the reason for the reported effectiveness of this nudge may be tied to who the account holder was. Using Vanessa, the account holder who appears to be an elderly woman, may have been a factor when it came to nudging people to be more honest. This was hinted at in the earlier extract/quotation from Participant 3. Choosing a different account holder persona could have affected the

nudge's effectiveness; i.e., made it more or less effective. Another issue with using an elderly "Vanessa" is that a few instances or responses suggested that her age might paint her as a more vulnerable target.

R: "Okay. So, okay. So, to criminal Jack, what stood out was the name. The account number and the picture, what else?"

P5: "Picture. And that she's a bit older. So, she'd be less likely to catch on to what's happening."

Participant 5 (Male, 47, Bachelor's Degree)

Arfi and Agarwal (2013) and Zulkipli et al. (2021) also found that cybercriminals may target the elderly due to a lack of cybersecurity awareness. Overall, while very helpful in discouraging fraudulent behaviour, the instigate empathy nudge mechanism is not perfect.

7.5.3 Opportunism and Justification in the Digital Context

As mentioned earlier at the start of this section, this final theme focused on the rationalisations used to justify committing online banking fraud. Subsequently, these are the factors or reasons behavioural interventions targeting COM-B factors hope to alter or make more difficult to use. It is split into two subthemes: "Justification-biased logic" and "Digital context and perception of risk". This section focuses on helping to answer the third research question.

7.5.3.1 Digital Context and Risk

As mentioned in Section 6.5.9, a significant aspect of the digital context involved the fear of being tracked down via all the digital "breadcrumbs" left when interacting with an online banking website. This differentiates it from the other contexts in which a third party may have an opportunity to steal another person's money, such as picking up someone's wallet. In most responses, the risk of being tracked was a major factor that had to be considered. Third parties, in such scenarios, may fear the "trail of breadcrumbs" that could be used to track and subsequently punish a third party for committing fraud. This ties into the deterrence theory mentioned in Section 7.5.1.2 as the potential threat of punishment in itself helps to prevent people from committing online banking fraud. It is worth noting that the risk alone is not always enough reason

not to commit online banking fraud, as some individuals may be willing to take that risk.

When on an online banking website, anything that gives the impression of greater security helps to dissuade online banking fraud. This could be employed when designing nudges for online banking websites. As mentioned in Section 7.3, the most effective nudges on the PRE-LOG version of the website had a general focus on creating the impression of enhanced security and more granular transaction monitoring. Li and Luo (2012) employed something similar in the context of combatting social engineering, which they called constructive deception. Their study investigated controlling what information was shared with which stakeholder. As implied by the term “constructive deception”, some cases involved actively deceiving stakeholders who lacked the required authorisation or permissions regarding restricted information and procedures of an organisation. The goal was to make it harder for malicious actors like social engineers to gain accurate information regarding the organisation’s procedures and security, which makes successful attacks less likely. In the context of online banking, informing users of the website about the security measures protecting accounts is useful. Still, it may also be helpful to exaggerate the capability and effectiveness of employed security measures. However, the extent to which exaggeration is employed may have to be tempered a bit, as some more tech-savvy third parties may be able to spot the deception if it seems too far-fetched. Overall, manipulating the choice architecture to create the perception of greater security can help dissuade online banking fraud.

7.5.3.2 Justification-Biased Logic

This theme focused on the use of biased and self-serving rationalisations a third party may use to and thus rationalise committing online banking fraud. Overall, as mentioned in Section 6.6, there were approximately nine rationalisations; thus helping to answer the third research question.

(a) Down on Their Luck

A third party in a similar scenario may use any recent misfortune or financial setbacks they experienced to help justify committing online banking fraud. In the scenario provided, this would be a car accident and subsequent repair costs that need to be

covered. This suggests that third parties in dire financial straits at the time are more likely to be tempted to commit online banking fraud than others. The high number of occurrences of this fraud-enabling rationalisation suggests that many third parties may use such a rationalisation when committing fraud. Around eight participants brought up something to do with this rationalisation.

(b) Lack of Observers in the Area

A part of the scenario in all three versions, and subsequently the hypothetical opportunity to commit online banking fraud, was the assumption that the third party was alone near the computer with the credentials. As it turns out, this could help encourage fraud as a third party may believe they can commit the act and get away with it. This is similar to the fear of tracking in the digital context but instead looks at the more traditional idea of witnesses to a crime. It can also be tied to the threat of punishment theme discussed earlier, both from the legal and social side; in other words, a witness can help authorities to prosecute a third party, or the negative impact on their social reputation from being labelled a thief. However, this fraud-enabling rationalisation was still on the rare side, being brought up by only two participants and only in the Control version.

(c) Greed

Where the “Down on their luck” rationalisation looked at someone who may be struggling financially and using that as an excuse, this rationalisation suggests that people may simply want more money and wealth. In other words, even when they are doing well, a third party may commit online banking fraud simply because they want more. Such cases imply a lack of remorse for their actions, as an individual does not seem to need a reason to help justify stealing from someone else, despite any laws or social norms condemning it. This can be linked to the situational cue of financial incentives brought up by multiple studies (Gneezy et al., 2018; Gerlach et al., 2019). However, the size of the incentive itself did not seem to be a factor. While the fraud-enabling rationalisation itself is unsurprising, what was surprising was how rarely it came up, and it only really came up in one interview.

(d) Sunk Cost Fallacy and Curiosity

A relatively common idea among the participants was that people would explore the website first. A third party visiting the website may not immediately log out or attempt to transact or tamper with an account. As the former implies, this exploration is not always motivated by malice or typical greed, and individuals may log out without causing financial harm. Where curiosity may cause an issue is when an individual may fall victim to the sunk cost fallacy. In such a case, a third party may decide simply because of all the steps already taken thus far that they might as well go “all the way” and commit online banking fraud; i.e., “I have already used someone else’s credentials to log in, which is wrong, so I might as well also get some money”. This is similar to the findings of Amigud and Lancaster (2019) and Gravert (2013), who found that prior effort exerted was often used to justify dishonest behaviour. While “sunk cost” was a relatively rare fraud-enabling rationalisation in isolation, it became one of the most common when combined with curiosity. Across all three versions, approximately six participants’ responses involved an element of “sunk cost fallacy” and “curiosity”.

(e) Overconfidence and Lower Perceived Risk of Detection

As implied earlier in the “Digital context and risk” subsection, perceived risk of detection helps to dissuade online banking fraud. On the other hand, a lower perceived detection risk helps an individual to rationalise committing fraud. This rationalisation dealt with the idea that individuals may have believed their chances of evading detection to be extremely high without sufficient information supporting it or even with information to the contrary. In simple terms, some third parties may be unreasonably confident regarding their chances of escaping detection and thus decide to commit online banking fraud. A similar bias was found in other studies for both nudging (Mongin and Cozic, 2014; Acquisti et al., 2017) and deterrence theory (Piquero et al., 2011). This rationalisation significantly overlaps with “Digital context and perception of risk”. A relatively common fraud-enabling rationalisation arose during the interviews with four participants.

(f) Inherent Dishonest Nature

The idea of inherent nature dictates how people responded to similar scenarios where there was an opportunity to commit fraud. Some third parties, by their nature, may lean towards a more dishonest nature and subsequently have fewer qualms about

committing fraud. Such individuals are closer to the Will hypothesis brought up by Amigud and Lancaster (2019) and Speer et al. (2020). Changing the behaviour of such individuals would be much more difficult, which suggests instances where nudging may be of limited use, as their focus would be on what they could gain from the opportunity. While the question of intrinsic nature often arose, only three participants explicitly brought up this fraud-enabling “side of the coin”.

(g) Accessing an Open Account Is Not That Bad

Part of the scenario design, especially in the POST-LOG version, was that a third party would stumble upon someone else’s online banking credentials. This could be used as a potential rationalisation as there was no active breach or search for the account holder’s credentials. This could be used to reduce any negative impact on their self-image, as they positively compared themselves to cybercriminals. To some extent, this was an example of the theory of self- concept maintenance described by Mazar et al. (2008), Ariely (2012), Gneezy et al. (2018), and Shalvi et al. (2015). Given how common this theory is in the literature, it was surprising that this rationalisation was only mentioned by two participants.

(h) Crime of Opportunity

In general, a third party may take advantage of similar opportunities because they are rare to come across. There is little planning beforehand, but they may still use such an opportunity to enrich themselves. This can also be linked to the lack of observers, as public venues such as Internet cafés often have other people in them. Being brought up by six participants, this rationalisation was easily one of the most common.

(i) Hurt Them Because of Their Mistakes

Someone may decide to commit online banking fraud to teach the account holder about the risk of being negligent with the security of their bank account. This justification also involves blaming the victim rather than taking accountability for online banking fraud. Two participants brought up this rationalisation, but interestingly enough, it did not come up in the literature review.

Based on the number of participants who brought up concepts and ideas related to the respective rationalisations, they were ranked from the most common to the least common in Table 7.1.

Table 7.1: Rationalisations ranked

| Rationalisations | No. of participants who mentioned it | Ranking |
|--|---|----------------|
| Crime of opportunity | 6 | 1 |
| Down on their luck | 6 | 1 |
| Sunk cost fallacy and curiosity | 6 | 1 |
| Overconfidence and lower perceived risk of detection | 4 | 4 |
| Inherent dishonest nature | 3 | 5 |
| Lack of observers in the area | 2 | 6 |
| Accessing an open account is not that bad | 2 | 6 |
| Greed | 1 | 7 |

7.6 Summary

This chapter focused on discussing the findings from the previous chapter in relation to how they helped to answer the study's research questions. The study found that the most effective nudging mechanisms are tied to increasing the perceived security of the website and instigating empathy by personalising clients' accounts. Of the two mechanisms, personalisation was found to be more effective. Overall, the best place to implement nudges is after logging in to an online banking account rather than before. To help answer the final research question, a variety of rationalisations a third party could use to commit fraud were discussed. The subsequent chapter focuses on the conclusions of this study.

CHAPTER 8:

CONCLUSION

8.1 Introduction

This final chapter explains the conclusions reached based on the analysis and discussion of the study's findings. It links these conclusions to the research problem and the research questions as discussed in Chapter 1.

8.2 Problem Description Revisited

Online banking has existed for several years and is a service that most banks offer. Online banking offers added convenience by allowing a bank's clients to access their accounts remotely. However, like other forms of banking, the threat of fraud is also present in this online context and is a significant concern. Banks have invested in various traditional cybersecurity measures to help address these concerns. However, incidences of online banking fraud still occur, which result in significant financial losses for them and their clients. Human error via the bank's clients may compromise their online banking credentials. When this happens, there is a chance for someone who is neither the account holder nor a bank representative (i.e., a third party) to stumble upon the compromised credentials. In such scenarios, the third party may be tempted to exploit the compromised credentials and commit online banking fraud by making unauthorised transactions. This study's primary goal was to investigate how effective the behavioural intervention of nudging could be, specifically with regard to dissuading third parties from committing online banking fraud. The two secondary goals focused on where online banking website nudges should ideally be deployed and what rationalisations may be used to justify committing online banking fraud. The study's research questions stemmed from these goals (see Section 1.4).

8.3 Research Questions Revisited

8.3.1 RQ1: Which choice architecture manipulations (“nudges”) are the most effective at dissuading online banking fraud?

Overall, the most effective group of nudges focused on encouraging empathy in the individual currently using the website by personalising the online banking website interface. Based on participants’ responses, an authorised third party was more likely to feel guilty for transacting on someone else’s account when they could more clearly imagine the victim. They may decide not to commit online banking fraud to avoid this guilt.

Given the digital context of online banking, another group of nudges that was very effective in dissuading online banking fraud focused on increasing the perception of online banking security measures. The participants’ responses to the rationalisation interview questions suggested that this increase in perceived security also increases the perceived risk of being tracked down and subsequently punished for committing online banking fraud. Making the inherent tracking risk of the digital context of online banking seem greater helps to dissuade individuals from committing online banking fraud, as they fear they are more likely to face the consequences of being caught, both legally and socially.

8.3.2 RQ2: When comparing the placement of nudges before and after logging in, where is it more effective to deploy nudging to dissuade online banking fraud?

Employing nudges after someone has logged in to an online banking account is more effective than employing them before they have logged in. Employing nudges before and after logging in yields little additional benefit in dissuading online banking fraud, which suggests that after logging in should be the main area an online banking website should focus on if implementing nudges.

8.3.3 RQ3: If a third party impersonates or defrauds the legitimate account holder, how do these individuals rationalise their dishonest actions?

The findings indicated that individuals use selfish or biased reasoning to help them rationalise committing online banking fraud. Generally, in descending order in terms of how common they were, these rationalisations included the following:

- Crime of opportunity;
- Down on their luck;
- Sunk cost fallacy and curiosity;
- Overconfidence and lower perceived risk of detection;
- Hurt them because of their mistakes;
- Accessing an open account is not that bad;
- Individual's inherent dishonest nature;
- Lack of observers in the area; and
- Greed.

The most common aspect that arose from the participants' responses was the perceived risk of tracking being acceptable, which makes taking advantage of the opportunity to commit fraud easier.

8.4 Methodological Approach Used

This study used an interpretivist research paradigm and the COM-B model of behaviour change as its framework. These were combined and used as part of a larger experiment-based research strategy. The COM-B model suggests that for any intervention to change an individual's behaviour successfully, it must change one or more of three factors preceding the behaviour. These factors are capability (C), opportunity (O), and motivation (M). In the context of this study, employing nudges was meant to target one or more of these factors by making it more difficult for a third party to rationalise committing online banking fraud. To investigate the nudges and to discover some of the rationalisations that a third party might use, semi-structured interviews were conducted, during which the participants could interact with three versions of a fictional online banking website. These interviews were transcribed and

thematically analysed. Using the resultant thematic maps, the study's findings helped to answer the research questions.

8.5 Research Contribution

This study extends the body of knowledge surrounding the behavioural use of nudging and its potential applications in various contexts; in particular, to dissuade online banking fraud, which is a previously unexplored application thereof in the field of cybersecurity. Nudges that instigate empathy with the original account holder or increase the perception of security were found to be the most effective to dissuade online banking fraud. This study also demonstrated how the COM-B model of behaviour change can be used to theoretically frame the application of said nudging theory and related choice architecture manipulations to study dishonest behaviours. Although most nudges can be mapped onto the capability factor, some mechanisms are exceptions to this and overlap with the motivation and opportunity factors of the COM-B model. The final contribution is to dishonesty-related literature, as it helps to expand the understanding of how honesty could be encouraged in individuals. Several rationalisations that could be used to justify or prevent individuals from committing fraud were discovered in this study. The justifications used to rationalise fraud were compared and ranked in terms of how many participants in the interview sample mentioned something linked to the rationalisation.

8.6 Implications for Theory

Empathy and personalisation could be powerful motivators for encouraging more honest or ethical behaviour, potentially in other contexts that move beyond fraud. This is in line with similar findings by Ariely (2012) and Cohn et al. (2019). Even in a context like online banking, which is traditionally very impersonal and focused on providing a service, personalisation could be useful to discourage dishonest or unethical behaviour.

The perception of the security of a digital or online system may be an important factor in terms of how it deters potential intrusion(s) or cyberattack(s). Whether or not this can be incorporated into future cybersecurity models and theories remains to be seen; at least within the literature reviewed.

The phenomenon noted in the guilt aversion hypothesis may also involve fear of punishment; thus linking it to what is suggested by the deterrence theory. The link between social sanctions and guilt aversion can be explored in future research as guilt aversion's effect on behaviour may go beyond only causing discomfort or stress caused by not meeting the perceived ethical standards of their social group (Chang et al., 2011; Khalmetski, 2016).

8.7 Implications for Practice

Constructive deception can potentially be employed to help protect organisations' information systems, as threat actors operate on incomplete or inaccurate information (Li and Luo, 2012). Rather than relying on omission, exaggeration may also be helpful when it comes to constructive deception by cybersecurity defence actors. This gives cybersecurity professionals an additional option to protect their organisation's digital systems.

Nudges can potentially supplement traditional security measures already employed in online banking. Designing the interfaces of such websites may be worthwhile researching and incorporating the findings from digital nudging research. This could advocate for its addition to the suite of the cybersecurity measures organisations already use. If behavioural interventions could potentially work in the context of online banking, then they could apply or be explored in other cybersecurity contexts. At the same time, by not restricting options, nudges are relatively unobtrusive for end users.

8.8 Limitations and Future Research

This study was not without its limitations. Firstly, the limited sample size of 15 was a very small proportion of the overall population of online banking users. Any future research should use larger samples, as they may discover new things not found in this study. Also linked to the sample, another limitation arose from the sample recruited. Recruiting exclusively from the USA may have affected how well the findings can be generalised to other countries. Subsequently, future research should explore if the findings of this study could still apply in other countries, given any sociocultural differences and cybersecurity measures employed by their banks.

The participants were aware of the experiment throughout their interactions with the websites; there was thus the risk that some may have given socially desirable responses rather than what they would actually do in the provided scenarios. The role-play and scenario aspects (What do you think Jack/Jill ...) were implemented to help mitigate this issue, but it was not perfect. To help gain a sense of how applicable nudging is “out in the wild”, future research could potentially look at testing nudging in experiments where participants are unaware that it has been employed to dissuade fraud. Tied to deploying nudging in a real-world cybersecurity scenario, another limitation was the implicit assumption that nudging would be significantly less effective when the account holder was targeted. In other words, when no accident or user error leads to compromised credentials and vulnerable accounts, but rather they are targeted by cybercriminal(s). This assumption should also be tested in future research to verify if this assumption was correct, as such scenarios of online banking fraud could be more likely to occur than those used within this study (i.e. average third party or a random third party). Recruiting participants in such a study may be more difficult, but if this assumption is validated, it could significantly affect how reliable banks may find this study’s findings.

Linked to the cybercriminal assumption and hinted at earlier in Figure 6.11 in Chapter 6.5, an individual’s inherent moral nature could significantly affect how they would respond to a similar scenario they encountered. As a result, some participants may have had a more difficult time trying to role-play or imagine the rationalisations that someone who was very (dis)honest would have done in such a scenario. In other words, their individual differences and moral frameworks could ‘colour’ how they believed a third party would respond in the scenario. Participants who are cybercriminals may skew towards the inherently dishonest. Thus further studies involving them specifically could help ‘paint a better picture’ of the effectiveness of nudges. Without looking at such instances, it makes it harder to gauge how reliable the results of this study could be ‘out in the wild’ as such malicious actors are more likely to be the cause of online banking fraud as compared to your average person simply walking by at the right time and place.

The final limitation concerns the website design itself. The fictional website developed for this study only attempted to replicate the look and some very limited functionality of online banking websites. UI design knowledge and best practice guidelines may

need to be considered when designing digital nudges and implementing them in online banking or other digital contexts. The intersection of digital nudging with UI design knowledge and skills could be explored in future research.

8.9 Summary of the Thesis

This study had three objectives it set out to achieve. Firstly, it set out to investigate the effectiveness of nudging in helping to dissuade online banking fraud. Secondly, it sought to discover where best to employ nudges on an online banking website and, finally, to discover some of the rationalisations an individual may use to help justify committing online banking fraud. Chapter 1 introduced the research problem and provided an overview of the study. Chapter 2 examined literature regarding existing security measures already employed by banks on their websites. Chapter 3 shifted the focus to the literature surrounding rationalisations and (dishonest) behaviour and introduced the COM-B model. Chapter 4 moved on to nudging to provide extra information regarding the behavioural intervention and the various mechanisms by which it may be employed. Chapter 5 outlined the research methodology employed by this study. This was followed by the findings and discussion chapters, which explored the results of the data analysis conducted for this study. Following them, this final chapter focused on explicitly answering the research questions and what the answers to those questions might imply for theory and practice. Overall, nudging can potentially be used to help dissuade online fraud. Given the potential financial impact of online banking fraud on banks and their clients, it should not be used as the sole defence to protect their clients. Rather, it should be used to help enhance or complement banks' pre-existing security measures and further reduce instances of online banking fraud.

REFERENCES

- Abeler, J., Nosenzo, D. and Raymond, C., 2019. Preferences for truth-telling. *Econometrica*, 87(4): 1115–1153. <https://doi.org/10.3982/ecta14673>.
- Acquisti, A., 2009. Nudging Privacy: The behavioral economics of personal information. *IEEE Security & Privacy*, 7(6): 82–85. [online] Available at: <<http://www.computer.org/portal/web/computingnow/1209/whatsnew/securityandprivacy%5Cnpapers2://publication/uuid/0B374D7F-D643-4BDF-8A20-D1B810BCAC3D>> [Accessed 4 April 2022].
- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y. and Wilson, S., 2017. Nudges for privacy and security: Understanding and assisting users' choices. *ACM Computing Surveys*, 50(3): 1–41. <https://doi.org/10.1145/3054926>.
- Adams, A. and Sasse, M.A., 1999. Users are not the enemy. *Communications of the ACM*, 42(12): 41–46.
- Aguiler, M., 2015. *Here's Why Your Bank Account Is Less Secure Than Your Gmail*. [online] Available at: <<https://gizmodo.com/heres-why-your-bank-account-is-less-secure-than-your-gm-1683777281>> [Accessed 11 April 2021].
- Ahmad, I., Iqbal, S., Jamil, S. and Kamran, M., 2021. A systematic literature review of e-banking frauds: Current scenario and security techniques. *Linguistica Antverpiensia*, 2021(2): 3509–3517.
- Akhter, S.H., 2015. Impact of internet usage comfort and internet technical comfort on online shopping and online banking. *Journal of International Consumer Marketing*, 27(3): 207–219. <https://doi.org/10.1080/08961530.2014.994086>.
- Akhter, S. and Tariq, J., 2022. Customer retention for digital banking: Application of 'nudge theory'. *Bangladesh Journal of Integrated Thoughts*, 17(2): 19–38. <https://doi.org/10.52805/bjit.v17i2.243>.
- Alhabash, S., Mengtian, J., Brooks, B., Rifon, N.J., LaRose, R. and Cotten, S.R., 2015. Online banking for the ages: Generational differences in institutional and system trust. *Communication and Information Technologies Annual*, 10: 145–171.
- Alkassim, R.S. and Tran, X., 2016. Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1): 1–4. <https://doi.org/10.11648/j.ajtas.20160501.11>.

- American Banking Association, 2022. Study: Banks see rise in fraud attempts, associated costs in 2021. *ABA Banking Journal*, 6 January. [online] Available at: <<https://bankingjournal.aba.com/2022/01/study-banks-see-rise-in-fraud-attempts-associated-costs-in-2021/>> [Accessed 25 November 2022].
- Amigud, A. and Lancaster, T., 2019. 246 reasons to cheat: An analysis of students' reasons for seeking to outsource academic work. *Computers and Education*, 134(January): 98–107. <https://doi.org/10.1016/j.compedu.2019.01.017>.
- Aquino, K., Freeman, D., Reed, A., Lim, V.K.G. and Felps, W., 2009. Testing a social-cognitive model of moral behavior: The interactive influence of situations and moral identity centrality. *Journal of Personality and Social Psychology*, 97(1): 123–141. <https://doi.org/10.1037/a0015406>.
- Arfi, N. and Agarwal, S., 2013. Knowledge of cybercrime among elderly. *International Journal of Scientific and Engineering Research*, 4(7): 1463–1468. [online] Available at: <<http://www.ijser.org/researchpaper/Knowledge-of-Cybercrime-among-Elderly.pdf>> [Accessed 8 January 2022].
- Ariely, D., 2012. *The (Honest) Truth About Dishonesty: How We Lie to Everyone—Especially Ourselves*. EPub ed. London: Harper Collins Publishers. <https://doi.org/10.1080/10999922.2015.1064693>.
- Axure Software Solutions, 2022. *Axure RP – UX Prototypes, Specifications, and Diagrams in One Tool*. [online] Available at: <<https://www.axure.com/>> [Accessed 23 May 2022].
- Bahl, S., 2012. E-Banking: Challenges & policy implications. *International Journal of Computing & Business Research*, 2229–6166.
- Bănărescu, A., 2015. Detecting and preventing fraud with data analytics. *Procedia Economics and Finance*, 32(15): 1827–1836. [https://doi.org/10.1016/s2212-5671\(15\)01485-9](https://doi.org/10.1016/s2212-5671(15)01485-9).
- Barker, F., Atkins, L. and De Lusignan, S., 2016. Applying the COM-B behaviour model and behaviour change wheel to develop an intervention to improve hearing-aid use in adult auditory rehabilitation. *International Journal of Audiology*, 55: S90–S98. <https://doi.org/10.3109/14992027.2015.1120894>.

- Barton, A. and Grüne-Yanoff, T., 2015. From libertarian paternalism to nudging—and beyond. *Review of Philosophy and Psychology*, 6(3): 341–359. <https://doi.org/10.1007/s13164-015-0268-x>.
- Batson, C.D., Thompson, E.R. and Chen, H., 2002. Moral hypocrisy: Addressing some alternatives. *Journal of Personality and Social Psychology*, 83(2): 330–339. <https://doi.org/10.1037/0022-3514.83.2.330>.
- Battigall, P. and Dufwenberg, M., 2007. Guilt in games. *The American Economic Review*, 97(2): 170–176.
- Bazerman, M.H. and Gino, F., 2012. Behavioral ethics: Toward a deeper understanding of moral judgment and dishonesty. *Annual Review of Law and Social Science*, 8: 85–104. <https://doi.org/10.1146/annurev-lawsocsci-102811-173815>.
- Belás, J., Korauš, M. and Gabčová, L., 2015. Electronic banking, its use and safety: Are there differences in the access of bank customers by gender, education and age? *International Journal of Entrepreneurial Knowledge*, 3(2): 16–28. <https://doi.org/10.1515/ijek-2015-0013>.
- Belás, J., Korauš, M., Kombo, F. and Korauš, A., 2016. Electronic banking security and customer satisfaction in commercial banks. *Journal of Security and Sustainability Issues*, 5(3): 411–422. [https://doi.org/10.9770/jssi.2016.5.3\(9\)](https://doi.org/10.9770/jssi.2016.5.3(9)).
- Bennett, M.J., 1979. Overcoming the golden rule: Sympathy and empathy. *Annals of the International Communication Association*, 3(1): 407–422. <https://doi.org/10.1080/23808985.1979.11923774>.
- Berger, S.C. and Gensler, S., 2007. Online banking customers: Insights from Germany. *Journal of Internet Banking and Commerce*, 12(1): 1–6. [online] Available at: <<https://www.icommercecentral.com/open-access/online-banking-customers-insights-from-germany.php?aid=38482&view=mobile>> [Accessed 19 October 2022].
- Boddy, C.R., 2016. Sample size for qualitative research. *Qualitative Market Research*, 19(4): 426–432. <https://doi.org/10.1108/QMR-06-2016-0053>.
- Boothroyd, V. and Chiasson, S., 2013. Writing down your password: Does it help? *Proceedings of the 2013 11th Annual Conference on Privacy, Security and Trust (PST 2013)*. Spain: IEEE. pp. 267–274. <https://doi.org/10.1109/PST.2013.6596062>.

- Botacin, M., Kalysch, A. and Grégio, A., 2019. The internet banking [in]security spiral: Past, present, and future of online banking protection mechanisms based on a Brazilian case study. *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1–10. <https://doi.org/10.1145/3339252.3340103>.
- Braun, V. and Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2): 77–101. <https://doi.org/10.1191/1478088706qp0630a>.
- Broers, V.J.V., De Breucker, C., Van den Broucke, S. and Luminet, O., 2017. A systematic review and meta-analysis of the effectiveness of nudging to increase fruit and vegetable choice. *European Journal of Public Health*, 27(5): 912–920. <https://doi.org/10.1093/eurpub/ckx085>.
- Buonanno, P., Pasini, G. and Vanin, P., 2012. Crime and social sanction. *Papers in Regional Science*, 91(1): 193–218. <https://doi.org/10.1111/j.1435-5957.2010.00349.x>.
- Bursztein, E., Benko, B., Margolis, D., Pietraszek, T., Archer, A., Aquino, A., Pitsillidis, A. and Savage, S., 2014. Handcrafted fraud and extortion: Manual account hijacking in the wild. *Proceedings of the ACM SIGCOMM Internet Measurement Conference*, pp. 347–358. <https://doi.org/10.1145/2663716.2663749>.
- Calo, R., 2014. Code, nudge, or notice? *Iowa Law Review*, 99(2): 773–802.
- Caraban, A., Karapanos, E., Gonçalves, D. and Campos, P., 2019. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. *Proceedings of the Conference on Human Factors in Computing Systems*, pp. 1–15. <https://doi.org/10.1145/3290605.3300733>.
- Cartwright, E., 2019. Guilt aversion and reciprocity in the performance-enhancing drug game. *Journal of Sports Economics*, 20(4): 535–555. <https://doi.org/10.1177/1527002518794793>.
- Cassim, F., 2010. Addressing the challenges posed by cybercrime: A South African perspective. *Journal of International Commercial Law and Technology*, 5(3): 118–123.
- Castleman, B.L. and Page, L.C., 2015. Summer nudging: Can personalized text messages and peer mentor outreach increase college going among low-income high school graduates? *Journal of Economic Behavior and Organization*, 115: 144–160. <https://doi.org/10.1016/j.jebo.2014.12.008>.

- Chang, L.J., Smith, A., Dufwenberg, M. and Sanfey, A.G., 2011. Triangulating the neural, psychological, and economic bases of guilt aversion. *Neuron*, 70(3): 560–572. <https://doi.org/10.1016/j.neuron.2011.02.056>.
- Cherry, K., 2021. *What Is the Representativeness Heuristic?* [online] Available at: <<https://www.verywellmind.com/representativeness-heuristic-2795805>> [Accessed 4 November 2021].
- Choe, E.K., Jung, J., Lee, B. and Fisher, K., 2013. Nudging people away from privacy-invasive mobile apps through visual framing. In P. Kotzé, G. Marsden, G. Lindgaard, J. Wesson and M. Winckler, eds. *Human-Computer Interaction – INTERACT 2013: Lecture Notes in Computer Science*, vol. 8119. Berlin: Springer. pp. 74–91. https://doi.org/10.1007/978-3-642-40477-1_5.
- Choubey, J. and Choubey, B., 2013. Secure user authentication in internet banking: A qualitative survey. *International Journal of Innovation, Management and Technology*, 4(2): 198–203. <https://doi.org/10.7763/ijimt.2013.v4.391>.
- Claessens, J., Valentin, D., De Cock, D., Preneel, B. and Vandewalle, J., 2002. On the security of today's online electronic banking systems. *Computers & Security*, 21(3): 253–265.
- Clark, D., 2021. *Value of Annual Online Banking Fraud Losses*. [online] Available at: <<https://www.statista.com/statistics/326169/united-kingdom-uk-online-banking-losses/>> [Accessed 10 March 2021].
- Cohn, A., Maréchal, M.A., Tannenbaum, D. and Zünd, C.L., 2019. Civic honesty around the globe. *Science*, 365(6448): 70–73. <https://doi.org/10.1126/science.aau8712>.
- Colbert, Y., 2019. Why is this online banking security feature common in other countries, but not Canada? *CBC News*, 7 October. [online] Available at: <<https://www.cbc.ca/news/canada/nova-scotia/two-factor-verification-online-banking-security-1.5306052>> [Accessed 11 April 2021].
- Collins English Dictionary*, 2021. 'Third Party Definition and Meaning'. [online] Available at: <<https://www.collinsdictionary.com/dictionary/english/third-party>> [Accessed 24 March 2021].
- Costa, C.M., 2022. Nudging is the architecture of choice in the world of banking. *Journal of Contemporary Administration*, 25: 1–13.
- Cristina, T., Beatrice, C. and Florentina, P., 2008. E-banking: impact, risks, security. *Annals of the University of Oradea, Economic Science Series*, 17(4).

- Dang, D., 2022. *12 Stats About Banking Fraud to Make That Impacts Businesses*. [online] Available at: <https://entrepreneurshipfacts.com/12-stats-about-banking-fraud-to-make-that-impacts-businesses/#8_Online_banking_accounted_for_33_of_US_banks_fraud_costs_in_2021> [Accessed 25 November 2022].
- Desisa, A. and Beshah, T., 2014. Internet banking security framework: The case of Ethiopian banking industry. *HiLCoE Journal of Computer Science and Technology*, 2(2): 7–13.
- Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. 2012. Influencing behaviour: The mindspace way. *Journal of Economic Psychology*, 33(1): 264–277.
- Dzomira, S., 2014. Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions*, 4(2): 16–26. <https://doi.org/10.22495/rgcv4i2art2>.
- Eddy, M., 2019. Does two-factor authentication really make you safer? *PCMag*, 5 June. [online] Available at: <<https://www.pcmag.com/opinions/does-two-factor-authentication-really-make-you-safer>> [Accessed 11 April 2021].
- Egelman, S., Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N. and Cranor, L., 2011. Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Vancouver, 7–12 May. [online] Available at: <<https://www.nist.gov/publications/passwords-and-people-measuring-effect-password-composition-policies>> [Accessed 1 May 2022].
- Enofe, A.O., Abilogun, T., Omoolorun, A.J. and Elaiho, E., 2017. Bank fraud and preventive measures in Nigeria: An empirical review. *International Journal of Academic Research in Business and Social Sciences*, 7(7): 40–51. <https://doi.org/10.6007/ijarbss/v7-i7/3076>.
- Fatima, A., 2011. E-banking security issues – Is there a solution in biometrics? *Journal of Internet Banking and Commerce*, 16(2): 1–9. [online] Available at: <<https://www.proquest.com/docview/915652371>> [Accessed 1 May 2022].
- Fehr, E. and List, J.A., 2004. The hidden costs and returns of incentives-trust and trustworthiness among CEOs. *Journal of the European Economic Association*, 2(5): 743–771. <https://doi.org/10.1162/1542476042782297>.

- Florêncio, D., Herley, C. and Coskun, B., 2007. *Do strong web passwords accomplish anything?* Paper presented at the 2nd USENIX Workshop on Hot Topics in Security, HotSec 2007. [online] Available at: <https://www.usenix.org/legacy/event/hotsec07/tech/full_papers/florencio/florencio.pdf> [Accessed 10 March 2021].
- Florêncio, D., Herley, C. and Van Oorschot, P., 2014a. An administrator's guide to internet password research. In *Proceedings of the 28th Large Installation System Administration Conference (LISA14)*, pp. 33–52. [online] Available at: <<https://www.usenix.org/conference/lisa14/conference-program/presentation/florencio>> [Accessed 14 June 2022].
- Florêncio, D., Herley, C., and Van Oorschot, P.C., 2014b. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *Proceedings of the 23rd USENIX Security Symposium*. [online] Available at: <<http://uml.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=c8h&AN=127096538&site=ehost-live>> [Accessed 8 January 2022].
- Franco, Z., 2018. *Choice Architecture: Introduction to Designing for Decision Making*. [online] Available at: <<https://medium.com/@Zekefranco/choice-architecture-introduction-to-designing-for-decision-making-3c2fd32cbc32>> [Accessed 10 March 2021].
- French, A.M., 2012. A case study on e-banking security: When security becomes too sophisticated for the user to access their information. *Journal of Internet Banking and Commerce*, 17(2): 2–14.
- Gabudeanu, L., Brici, I., Mare, C., Mihai, I.C. and Scheau, M.C., 2021. Privacy intrusiveness in financial-banking fraud detection. *Risks*, 9(6): 104. <https://doi.org/10.3390/risks9060104>.
- Gächter, S. and Schulz, J.F., 2016. Intrinsic honesty and the prevalence of rule violations across societies. *Nature*, 531: 496–499. <https://doi.org/10.1038/nature17160>.
- Gatsou, C., Politis, A. and Zevgolis, D., 2017. Seniors' experiences with online banking. In *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS 2017)*, 11: 623–627. <https://doi.org/10.15439/2017F57>.

- Gehring, E.F., 2002. Choosing passwords: Security and human factors. In *Proceedings of the IEEE 2002 International Symposium on Technology and Society (ISTAS'02): Social Implications of Information and Communication Technology*, pp. 369–373. <https://doi.org/10.1109/ISTAS.2002.1013839>.
- Gerlach, P., Teodorescu, K. and Hertwig, R., 2019. The truth about lies: A meta-analysis on dishonest behavior. *Psychological Bulletin*, 145(1): 1–44. <https://doi.org/10.1037/bul0000174>.
- Giles, J., 2010. The problem with online banking. *New Scientist*, 205(2745): 18–19. [https://doi.org/10.1016/S0262-4079\(10\)60224-2](https://doi.org/10.1016/S0262-4079(10)60224-2).
- Global Message Services, 2021. *Why is 2-Factor Authentication (2FA) So Important For Banks?* [online] Available at: <<https://www.gms-worldwide.com/blog/why-is-two-factor-authentication-2fa-so-important-for-banks/>> [Accessed 11 April 2021].
- Gneezy, U., Kajackaite, A., and Sobel, J., 2018. Lying aversion and the size of the lie. *The American Economic Review*, 108(2): 419–453.
- Gravert, C., 2013. How luck and performance affect stealing. *Journal of Economic Behavior and Organization*, 93: 301–304. <https://doi.org/10.1016/j.jebo.2013.03.026>.
- Gupta, A., 2006. Data protection in consumer e-banking. *Journal of Internet Banking and Commerce*, 11(1): 1–2.
- Hagman, W., Anderson, D., Vastfjall, D. and Tinghog, G., 2015. Public views on policies involving nudges. *Review of Philosophy and Psychology*, 6: 439–453.
- Hansen, P.G., 2016. The definition of nudge and libertarian paternalism: Does the hand fit the glove? *European Journal of Risk Regulation*, 7(1): 155–174. <https://doi.org/10.1017/S1867299X00005468>.
- Hargrave, L., 2021. *6 Common Types of Bank Accounts*. [online] Available at: <<https://www.creditkarma.com/advice/i/types-of-accounts>> [Accessed 20 July 2021].
- Hartl, V.M.I.A. and Schmuntzsch, U., 2016. Fraud protection for online banking: A user-centered approach on detecting typical double-dealings due to social engineering and inobservance whilst operating with personal login credentials. In T. Tryfonas, ed. *4th International Conference, HAS 2016, Held as Part of HCI International 2016, Toronto, ON, Canada, July 17-22, 2016, Proceedings*. https://doi.org/10.1007/978-3-319-39381-0_4.

- Hartwig, K. and Reuter, C., 2021. Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations. *Behaviour and Information Technology*, 41(7): 1357–1380.
- Helman, E., Stoller, R.M. and Freeman, J.B., 2015. Advanced mouse-tracking analytic techniques for enhancing psychological science. *Group Processes and Intergroup Relations*, 18(3): 384–401. <https://doi.org/10.1177/1368430214538325>.
- Heimerl, K., Menon, A., Hasan, S., Ali, K., Brewer, E. and Parikh, T., 2015. Analysis of smartphone adoption and usage in a rural community cellular network. *ACM International Conference Proceedings*, 15: 1–4. <https://doi.org/10.1145/2737856.2737880>.
- Hillman, J., 2022. *MTurk vs. Qualtrics vs. Prolific: Whose Survey Participants Are Best?* [online] Available at: <<https://www.prolific.co/blog/mturk-qualtrics-prolific-best-survey-participants>> [Accessed 18 October 2022].
- Hisamatsu, A., Pishva, D. and Nishantha, G.G.D., 2010. Online banking and modern approaches toward its enhanced security. In *International Conference on Advanced Communication Technology (ICACT)*. [online] Available at: <<https://dl.acm.org/doi/10.5555/1833006.1833114>> [Accessed 18 October 2022].
- Hoffmann, A.O.I. and Birnbrich, C., 2012. The impact of fraud prevention on bank-customer relationships. *International Journal of Bank Marketing*, 30(5): 390–407. <https://doi.org/10.1108/02652321211247435>.
- Hollingworth, C. and Barker, L., 2017. *BE360: Protecting Consumers from ‘Sludge’*. [online] Available at: <<https://www.research-live.com/article/features/be360-protecting-consumers-from-sludge/id/5031182>> [Accessed 20 July 2021].
- Holt, N., 2019. *Majority of People Return Lost Wallets*. [online] Available at: <https://theconversation.com/majority-of-people-return-lost-wallets-heres-the-psychology-and-which-countries-are-the-most-honest-119118?utm_medium=email...> [Accessed 4 April 2022].
- Horowitz, M., 2014. Financial firms not offering two factor authentication. *Computerworld*, 12 August. [online] Available at: <<https://www.computerworld.com/article/2476642/financial-firms-not-offering-two-factor-authentication.html>> [Accessed 18 October 2022].

- Howlett, N., Schulz, J., Trivedi, D., Troop, N. and Chater, A., 2019. A prospective study exploring the construct and predictive validity of the COM-B model for physical activity. *Journal of Health Psychology*, 24(10): 1378–1391. <https://doi.org/10.1177/1359105317739098>.
- Hummel, D. and Maedche, A., 2019. How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies. *Journal of Behavioral and Experimental Economics*, 80(September 2018): 47–58. <https://doi.org/10.1016/j.socec.2019.03.005>.
- Inglesant, P.G. and Sasse, M.A., 2010. The true cost of unusable password policies: Password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: Association for Computing Machinery. pp. 383–392. [online] Available at: <<https://doi.org/10.1145/1753326.1753384>> [Accessed 8 January 2022].
- Ioannou, A., Tussyadiah, I., Miller, G., Li, S. and Weick, M., 2021. Privacy nudges for disclosure of personal information: A systematic literature review and meta-analysis. *Plos One*, 16(8), e0256822. <https://doi.org/10.1371/journal.pone.0256822>.
- İşler, D., Küpçü, A. and Coskun, A., 2019. User perceptions of security and usability of mobile-based single password authentication and two-factor authentication. In C. Pérez-Solà, G. Navarro-Arribas, A. Biryukov and J. Garcia-Alfaro, eds. *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. New York: Springer International Publishing. pp. 99–117. [online] Available at: <<https://www.springerprofessional.de/en/user-perceptions-of-security-and-usability-of-mobile-based-singl/17190860>> [Accessed 20 July 2021].
- Ivanova, I., 2021. How websites use ‘dark patterns’ to manipulate you. *CBS News*, 14 May. [online] Available at: <<https://www.cbsnews.com/news/manipulative-advertising-technology-dark-patterns/>> [Accessed 20 July 2021].
- Jager, J., Putnick, D.L. and Bornstein, M.H., 2017. More than just convenient: The scientific merits of homogeneous convenience samples. *Monographs of the Society for Research in Child Development*, 82(2): 13–30. <https://doi.org/10.1111/mono.12296>.

- Jeske, D., Coventry, L., Briggs, P. and Van Moorsel, A., 2014. Nudging whom how: IT proficiency, impulse control and secure behaviour. In *Personalizing Behavior Change Technologies CHI Workshop*, 27 April. [online] Available at: <http://nrl.northumbria.ac.uk/17996/1/Jeske_et_al_2014_CHI_Personalised_Nudges.pdf> [Accessed 12 January 2022].
- Jesse, M. and Jannach, D., 2021. Digital nudging with recommender systems: Survey and future directions. *Computers in Human Behavior Reports*, 3(December): 100052. <https://doi.org/10.1016/j.chbr.2020.100052>.
- Johnson, E.J., Shu, S.B., Dellaert, B.G.C., Fox, C., Goldstein, D.G., Häubl, G., Larrick, R.P., Payne, J.W., Peters, E., Schkade, D., Wansink, B. and Weber, E.U., 2012. Beyond nudges: Tools of a choice architecture. *Marketing Letters*, 23(2): 487–504. <https://doi.org/10.1007/s11002-012-9186-1>.
- Kahneman, D., 2003. Maps of bounded rationality: Psychology for behavioral economics. *The American Economic Review*, 93(5): 1449–1475.
- Kawagoe, T. and Narita, Y., 2014. Guilt aversion revisited: An experimental test of a new model. *Journal of Economic Behavior and Organization*, 102: 1–9. <https://doi.org/10.1016/j.jebo.2014.02.020>.
- Kawugana, A. and Faruna, F.S., 2018. Fraud prevention in the Nigerian banking industry. *IIARD International Journal of Banking and Finance Research*, 4(1): 32–48. [online] Available at: <www.iiardpub.org> [Accessed 4 April 2022].
- Kenton, W., 2020. *Third Party Definition*. [online] Available at: <<https://www.investopedia.com/terms/t/third-party.asp>> [Accessed 24 March 2021].
- Keyworth, C., Epton, T., Goldthorpe, J., Calam, R. and Armitage, C.J., 2020. Acceptability, reliability, and validity of a brief measure of capabilities, opportunities, and motivations (“COM-B”). *British Journal of Health Psychology*, 25(3): 474–501. <https://doi.org/10.1111/bjhp.12417>.
- Khalmetski, K., 2016. Testing guilt aversion with an exogenous shift in beliefs. *Games and Economic Behavior*, 97: 110–119. <https://doi.org/10.1016/j.geb.2016.04.003>.
- Köbis, N.C., Verschuere, B., Bereby-Meyer, Y., Rand, D. and Shalvi, S., 2019. Intuitive honesty versus dishonesty: Meta-analytic evidence. *Perspectives on Psychological Science*, 14(5): 778–796. <https://doi.org/10.1177/1745691619851778>.

- Koskela, H., 2000. 'The gaze without eyes': Video-surveillance and the changing nature of urban space. *Progress in Human Geography*, 24(2): 243–265. <https://doi.org/10.1191/030913200668791096>.
- Koskosas, I., 2011. E-banking security: A communication perspective. *Risk Management*, 13(1–2): 81–99. <https://doi.org/10.1057/rm.2011.3>.
- Kraemer-Mbula, E., Tang, P. and Rush, H., 2013. The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80(3): 541–555. <https://doi.org/10.1016/j.techfore.2012.07.002>.
- Kroeze, F.M., Machiori, D.R. and De Ridder, D.T.D., 2015. Nudging healthy food choices: A field experiment at the train station. *Journal of Public Health*, 38(2): e133–e137.
- Krol, K., Philippou, E., De Cristofaro, E. and Sasse, M.A., 2015. 'They Brought In The Horrible Key Ring Thing!' Analysing The Usability Of Two-Factor Authentication In UK Online Banking. [online] Available at: <<https://arxiv.org/abs/1501.04434>> [Accessed 1 May 2022].
- Kroll, T. and Stieglitz, S., 2021. Digital nudging and privacy: Improving decisions about self-disclosure in social networks. *Behaviour and Information Technology*, 40(1): 1–19. <https://doi.org/10.1080/0144929X.2019.1584644>.
- Kuhfuss, L., Préget, R., Thoyer, S. and Hanley, N., 2016. Nudging farmers to enrol land into agri-environmental schemes: The role of a collective bonus. *European Review of Agricultural Economics*, 43(4): 609–636. <https://doi.org/10.1093/erae/jbv031>.
- Kumari, J.P., 2017. A study of online banking usage among university academics. *International Journal of Arts and Commerce*, 5(5): 1–6. [online] Available at: <https://www.ijac.org.uk/images/frontImages/gallery/Vol._5_No._5/1._1-6.pdf> [Accessed 1 May 2022].
- Lee, L., 2019. Cybercrime has evolved: It's time cyber security did too. *Computer Fraud and Security*, 2019(6): 8–11. [https://doi.org/10.1016/S1361-3723\(19\)30063-6](https://doi.org/10.1016/S1361-3723(19)30063-6).
- Lee, M.C., 2009. Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, 8(3): 130–141. <https://doi.org/10.1016/j.eierap.2008.11.006>.

- Lembcke, T.B., Engelbrecht, N., Brendel, A.B. and Kolbe, L.M., 2020. To nudge or not to nudge: Ethical considerations of digital nudging based on its behavioral economics roots. In *Proceedings of the 27th European Conference on Information Systems – Information Systems for a Sharing Society (ECIS 2019)*. [online] Available at: <<http://hubscher.org/roland/courses/hf765/readings/Lembcke2019.pdf>> [Accessed 26 October 2022].
- Lewicki, R.J. and Stark, N., 1996. What is ethically appropriate in negotiations: An empirical examination of bargaining tactics. *Social Justice Research*, 9(1): 69–95. <https://doi.org/10.1007/BF02197657>.
- Li, Y. and Luo, X., 2012. Constructive deception in the workplace and beyond: A defensive social engineering approach. *Proceedings of 2019 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop*, 66: 37–39.
- Luguri, J. and Strahilevitz, L.J., 2021. Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1): 43–109. <https://doi.org/10.1093/jla/laaa006>.
- Ly, K., Zhao, M. and Soman, D., 2013. *A Practitioner's Guide to Nudging*. [online] Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2609347> [Accessed 21 October 2021].
- Mabunda, S., 2019. Cyber extortion, ransomware and the South African Cybercrimes and Cybersecurity Bill. *Statute Law Review*, 40(2): 143–154. <https://doi.org/10.1093/slr/hmx028>.
- Mannan, M. and Van Oorschot, P.C., 2007. Security and usability: The gap in real-world online banking. In *Proceedings New Security Paradigms Workshop*, pp. 1–14. <https://doi.org/10.1145/1600176.1600178>.
- Mayne, J., 2016. *The Capabilities, Opportunities and Motivation Behaviour-Based Theory of Change Model*. [online] Available at: <https://www.researchgate.net/publication/301701597_The_Capabilities_Opportunities_and_Motivation_Behaviour-Based_Theory_of_Change_Model> [Accessed 18 October 2022].
- Mazar, N., Amir, O. and Ariely, D., 2008. The dishonesty of honest people: A theory of self-concept maintenance. *Journal of Marketing Research*, 45(6): 633–644. <https://doi.org/10.1509/jmkr.45.6.633>.
- McCue, J., 2018. *Our Definition of Adulthood Is Changing*. [online] Available at: <<https://www.weforum.org/agenda/2018/07/how-ideas-of-adulthood-its-rights-and-responsibilities-are-changing-around-the-world>> [Accessed 26 October 2022].

- McLeod, S., 2014. *The Interview Research Method*. [online] Available at: <<https://www.simplypsychology.org/interviews.html>> [Accessed 18 October 2022].
- Mehlkop, G. and Graeff, P., 2010. Modelling a rational choice theory of criminal action: Subjective expected utilities, norms, and interactions. *Rationality and Society*, 22(2): 189–222. <https://doi.org/10.1177/1043463110364730>.
- Michie, S., Van Stralen, M.M. and West, R., 2011. The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, 6(1): 42. <https://doi.org/10.1186/1748-5908-6-42>.
- Mirsch, T., Lehrer, C. and Jung, R., 2017. Digital nudging: Altering user behavior in digital environments. In *Proceedings der 13 Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, pp. 634–648.
- Missaoui, C., Bachouch, S., Abdelkader, I. and Trabelsi, S., 2018. Who is reusing stolen passwords? An empirical study on stolen passwords and countermeasures. In A. Castiglione, F. Pop, M. Ficco and F. Palmieri, eds. *Cyberspace Safety and Security, CSS 2018, Lecture Notes in Computer Science, vol. 11161*. Cham: Springer. pp. 3–17. https://doi.org/10.1007/978-3-030-01689-0_1.
- Molnár, A. and Chaudhry, S.J., 2018. *The Lesser of Two Evils: Explaining a Bad Choice by Revealing the Choice Set*. [online] Available at: <<https://psyarxiv.com/8sdme/>> [Accessed 7 September 2021].
- Mongin, P. and Cozic, M., 2014. Rethinking nudges. *SSRN Electronic Journal*, October: 1–25. <https://doi.org/10.2139/ssrn.2529910>.
- Mooijman, M., Meindl, P., Meindl, P., Oyserman, D., Monterosso, J., Dehghani, M., Doris, J.M. and Graham, J., 2018. Resisting temptation for the good of the group: Binding moral values and the moralization of self-control. *Journal of Personality and Social Psychology*, 115(3): 585–599. <https://doi.org/10.1037/pspp0000149>.
- Moore, T., Clayton, R. and Anderson, R., 2009. The economics of online crime. *Journal of Economic Perspectives*, 23(3): 3–20. <https://doi.org/10.1257/jep.23.3.3>.
- More, M.M., Jadhav, M.P. and Nalawade, K.M., 2015. Online banking and cyber attacks: The current scenario. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(12): 743–749.

- Mouton, F., Leenen, L. and Venter, H.S., 2016. Social engineering attack examples, templates and scenarios. *Computers and Security*, 59: 186–209. <https://doi.org/10.1016/j.cose.2016.03.004>.
- Mouton, F., Malan, M.M., Leenen, L. and Venter, H.S., 2014. Social engineering attack framework. In *Proceedings of the 2014 Information Security for South Africa (ISSA 2014) Conference*, pp. 1–9. <https://doi.org/10.1109/ISSA.2014.6950510>.
- Münscher, R., Vetter, M. and Scheuerle, T., 2016. A review and taxonomy of choice architecture techniques. *Journal of Behavioral Decision Making*, 29(5): 511–524. <https://doi.org/10.1002/bdm.1897>.
- Nagatsu, M., 2015. Social nudges: Their mechanisms and justification. *Review of Philosophy and Psychology*, 6: 481–494. <https://doi.org/10.1007/s13164-015-0245-4>.
- Natter, E., 2019. *Online Banking Disadvantages*. [online] Available at: <<https://smallbusiness.chron.com/online-banking-disadvantages-2248.html>> [Accessed 7 September 2021].
- Nilsson, M., Adams, A. and Herd, S., 2005. Building security and trust in online banking. In *Proceedings of the Conference on Human Factors in Computing Systems*, pp. 1701–1704. <https://doi.org/10.1145/1056808.1057001>.
- North, R., 2020. *What Are the Pros and Cons of Online Banking System*. [online] Available at: <<https://www.enterpriseedges.com/pros-cons-online-banking-system>> [Accessed 7 September 2021].
- Obar, J.A. and Oeldorf-Hirsch, A., 2020. The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information Communication and Society*, 23(1): 128–147. <https://doi.org/10.1080/1369118X.2018.1486870>.
- O'Hear, S., 2019. Prolific wants to challenge Amazon's Mechanical Turk in the online research space. *TechCrunch*, 4 December. [online] Available at: <<https://techcrunch.com/2019/12/04/prolific/>> [Accessed 18 October 2022].
- Omariba, Z.B., Masese, N.B. and Wanyembi, G., 2012. Security and privacy of electronic banking. *International Journal of Computer Science Issues*, 9(4): 432–446.

- Onaolapo, J., Mariconti, E. and Stringhini, G., 2016. What happens after you are pwnd: Understanding the use of leaked webmail credentials in the wild. *Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC)*, pp. 65–79. <https://doi.org/10.1145/2987443.2987475>.
- Osunmuyiwa, O., 2013. Online banking and the risks involved. *Research Journal of Information Technology*, 5(2): 50–54. <https://doi.org/10.19026/rjit.5.5787>.
- Petrykina, Y., Schwartz-Chassidim, H. and Toch, E., 2021. Nudging users towards online safety using gamified environments. *Computers and Security*, 108, 102270. <https://doi.org/10.1016/j.cose.2021.102270>.
- Phair, D. and Warren, K., 2021. *Saunders' Research Onion: Explained Simply (+ Examples)*. [online] Available at: <<https://gradcoach.com/saunders-research-onion/>> [Accessed 18 October 2022].
- Pilcher, J., 2020. *Infographic: The History Of Internet Banking (1983 - 2012)*. [online] Available at: <<https://thefinancialbrand.com/25380/yodlee-history-of-internet-banking/>> [Accessed 14 December 2020].
- Piquero, A.R., Paternoster, R., Pogarsky, G. and Loughran, T., 2011. Elaborating the individual difference component in deterrence theory. *Annual Review of Law and Social Science*, 7: 335–360. <https://doi.org/10.1146/annurev-lawsocsci-102510-105404>.
- Polumbo, B., 2019. 18 or 21? Time to make our mind up on the age of adulthood. *Washington Examiner*, 27 December. [online] Available at: <<https://www.washingtonexaminer.com/opinion/18-or-21-time-to-make-our-mind-up-on-the-age-of-adulthood>> [Accessed 26 October 2022].
- Raghavana, A.R. and Parthiban, L., 2014. The effect of cybercrime on a bank's finances. *International Journal of Current Research & Academic Review*, 2(2): 173–178.
- Renaud, K., 2021. Accessible cyber security: The next frontier? In *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP)*, pp. 9–18. <https://doi.org/10.5220/0010419500090018>.
- Renaud, K., Johnson, G. and Ophoff, J., 2020. Dyslexia and password usage: Accessibility in authentication design. In N. Clarke and S. Furnell, eds. *Human Aspects of Information Security and Assurance, HAISA 2020: IFIP Advances in Information and Communication Technology*, vol. 593. Cham: Springer. pp. 259–268. https://doi.org/10.1007/978-3-030-57404-8_20.

- Renaud, K. and Zimmermann, V., 2018. Ethical guidelines for nudging in information security & privacy. *International Journal of Human Computer Studies*, 120: 22–35. <https://doi.org/10.1016/j.ijhcs.2018.05.011>.
- Renaud, K. and Zimmermann, V., 2019. Nudging folks towards stronger password choices: Providing certainty is the key. *Behavioural Public Policy*, 3(02): 228–258. <https://doi.org/10.1017/bpp.2018.3>.
- Renaud, K., Zimmermann, V., Maguire, J. and Draper, S., 2017. Lessons learned from evaluating eight password nudges in the wild. In *2017 LASER Workshop – Learning from Authoritative Security Experiment Results*, pp. 25–37. [online] Available at: <<http://eprints.gla.ac.uk/153405/>> [Accessed 14 December 2020].
- Rosenbaum, S.M., Billinger, S. and Stieglitz, N., 2014. Let's be honest: A review of experimental evidence of honesty and truth-telling. *Journal of Economic Psychology*, 45: 181–196. <https://doi.org/10.1016/j.joep.2014.10.002>.
- Ruiz, R., Winter, R. and Amatte, F., 2017. The leakage of passwords from home banking sites: A threat to global cyber security? *Journal of Payments Strategy & Systems*, 11(2): 174–186.
- Saby, E., 2007. Barclays' smart approach to online fraud targets 0.5m customers. *Card Technology Today*, 19(4): 1. [https://doi.org/10.1016/s0965-2590\(07\)70062-2](https://doi.org/10.1016/s0965-2590(07)70062-2).
- Sanchez, M., 2019. Why you should never write down your passwords. *WhiteOut Press*, 15 March. [online] Available at: <<https://www.whiteoutpress.com/why-you-should-never-write-down-your-passwords/>> [Accessed 10 March 2021].
- Sarreal, R., 2019. *History of Online Banking: How Internet Banking Went Mainstream*. [online] Available at: <<https://www.gobankingrates.com/banking/banks/history-online-banking/>> [Accessed 14 December 2020].
- Saunders, M., Lewis, P. and Thornhill, A., 2016. *Research Methods for Business Students*. 7th ed. Harlow: Pearson Education.
- Schaer, A. and Stanoevska-Slabeva, K., 2019. Application of digital nudging in customer journeys – A systematic literature review. In *Proceedings of the 25th Americas Conference on Information Systems (AMCIS 2019)*, pp. 1–10.
- Schuchter, A. and Levi, M., 2013. The fraud triangle revisited. *Security Journal*, 29(2): 107–121. <https://doi.org/10.1057/sj.2013.1>.

- Scott, E.D. and Jehn, K.A., 2003. Multiple stakeholder judgments of employee behaviors: A contingent prototype model of dishonesty. *Journal of Business Ethics*, 46(3): 235–250. <https://doi.org/10.1023/A:1025529504435>.
- Segal, T., 2020. *Conflict of Interest Definition*. [online] Available at: <<https://www.investopedia.com/terms/c/conflict-of-interest.asp>> [Accessed 19 July 2021].
- Shah, S., Shah, B., Amin, A., Al-Obeidat, F., Chow, F., Moreira, F.J.L. and Anwar, S., 2019. Compromised user credentials detection in a digital enterprise using behavioral analytics. *Future Generation Computer Systems*, 93: 407–417. <https://doi.org/10.1016/j.future.2018.09.064>.
- Shalvi, S., Gino, F., Barkan, R. and Ayal, S., 2015. Self-serving justifications: Doing wrong and feeling moral. *Current Directions in Psychological Science*, 24(2): 125–130. <https://doi.org/10.1177/0963721414553264>.
- Shu, L.L. and Gino, F., 2012. Sweeping dishonesty under the rug: How unethical actions lead to forgetting of moral rules. *Journal of Personality and Social Psychology*, 102(6): 1164–1177. <https://doi.org/10.1037/a0028381>.
- Singh, N.P., 2020. Online frauds in banks with phishing. *Journal of Internet Banking and Commerce*, 2020. [online] Available at: <<https://www.icommercecentral.com/open-access/online-frauds-in-banks-with-phishing.php?aid=38493>> [Accessed 11 December 2020].
- Smith, A., 2012. 46% of American adults are smartphone owners phones within the national adult population. *Changes*, 1–9. [online] Available at: <<http://pewinternet.org/Reports/2012/Smartphone-Update-2012.aspx>> [Accessed 14 June 2022].
- Sood, A. and Enbody, R., 2011. The state of HTTP declarative security in online banking websites. *Computer Fraud and Security*, 2011(7): 11–16. [https://doi.org/10.1016/S1361-3723\(11\)70073-2](https://doi.org/10.1016/S1361-3723(11)70073-2).
- South African Banking Risk Information Centre, 2020. *Annual Crime Stats 2019*. [online] Available at: <<https://www.sabric.co.za/>> [Accessed 8 January 2022].
- Speer, S.P.H., Smidts, A. and Boksem, M.A.S., 2020. Cognitive control increases honesty in cheaters but cheating in those who are honest. *Proceedings of the National Academy of Sciences of the United States of America*, 117(32): 19080–19091. <https://doi.org/10.1073/pnas.2003480117>.

- Stobert, E., 2014. The agony of passwords: Can we learn from user coping strategies? In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '14. New York: Association for Computing Machinery, pp. 975–980. <https://doi.org/10.1145/2559206.2579421>.
- Stobert, E. and Biddle, R., 2014. The password life cycle: User behaviour in managing passwords. In *SOUPS '14: Proceedings of the Tenth Symposium on Usable Privacy and Security*, pp. 243–255.
- Story, P., Cranor, L.F., Smullen, D., Sadeh, N., Acquisti, A. and Schaub, F., 2020. From intent to action: Nudging users towards secure mobile payments. In *Proceedings of the 16th Symposium on Usable Privacy and Security, SOUPS 2020*. [online] (141), 1. Available at: <https://usableprivacy.org/static/files/story_soups_2020.pdf> [Accessed 1 May 2022].
- Sunstein, C.R., 2014. Nudging: A very short guide. *Journal of Consumer Policy*, 37(4): 583–588. <https://doi.org/10.1007/s10603-014-9273-1>.
- Sunstein, C.R., 2016. The council of psychological advisers. *Annual Review of Psychology*, 67: 713–737. <https://doi.org/10.1146/annurev-psych-081914-124745>.
- Sunstein, C.R., 2019. Sludge and Ordeals Forty-Ninth Annual Administrative Law Symposium: Deregulatory games: Essay. *Duke Law Journal*, 68(8): 1843–1884.
- Syniavska, O., Dekhtyar, N., Deyneka, O., Zhukova, T. and Syniavska, O., 2019. Security of e-banking systems: Modelling the process of counteracting fraud in e-banking. *SHS Web of Conferences*, 65: 03004. [online] Available at: <https://www.shs-conferences.org/articles/shsconf/abs/2019/06/shsconf_m3e22019_03004/shsconf_m3e22019_03004.html> [Accessed 1 May 2022].
- Syofyan, E., Pradini, D. and Kurniawati, T., 2017. The antecedents of fraud behavior: A finding from Indonesia. In *Proceedings of the Conference on Business Management 2017*, pp. 1494–1502. [online] Available at: <http://repository.unp.ac.id/38363/8/29c_similarity.pdf> [Accessed 1 May 2022].
- Thaler, R.H. and Sunstein, C.R., 2008. *Nudge: Improving Decisions About Health, Wealth and Happiness*. New Haven & London: Yale University Press.
- Tomlinson, K.D., 2016. An examination of deterrence theory: Where do we stand? *Federal Probation*, 80(3): 33–38.

- Turland, J., Coventry, L., Jeske, D., Briggs, P. and Van Moorsel, A., 2015. Nudging towards security: Developing an application for wireless network selection for Android phones. In *British HCI '15: Proceedings of the 2015 British HCI Conference*, pp. 193–201. <https://doi.org/10.1145/2783446.2783588>.
- United Nations Department of Economic and Social Affairs, 2019. *World Population Prospects 2019: Highlights*. [online] Available at: <https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/documents/2020/Jan/wpp2019_highlights.pdf> [Accessed 1 May 2022].
- Usman, A.K. and Shah, M.H., 2013. Critical success factors for preventing e-banking fraud. *Journal of Internet Banking and Commerce*, 18(2). [online] Available at: <<http://www.arraydev.com/commerce/jibc/>> [Accessed 14 June 2022].
- Verkijika, S.F., 2018. Factors influencing the adoption of mobile commerce applications in Cameroon. *Telematics and Informatics*, 35(6): 1665–1674. <https://doi.org/10.1016/j.tele.2018.04.012>.
- Vogel, G., 2004. The evolution of the golden rule. *Science*, 303(5661): 1128–1131. <https://doi.org/10.1126/science.303.5661.1128>.
- Wei, W., Li, J., Cao, L., Ou, Y. and Chen, J., 2013. Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web*, 16(4): 449–475. <https://doi.org/10.1007/s11280-012-0178-0>.
- West, R. and Michie, S., 2020. *A Brief Introduction to the COM-B Model of Behaviour and the PRIME Theory of Motivation*. <https://doi.org/10.32388/ww04e6.2>.
- Whitman, M.E. and Mattord, H.J., 2018. *Principles of Information Security*. 6th ed. Boston: Cengage Learning.
- Wijland, R., Hansen, P. and Gardezi, F., 2016. Mobile nudging: Youth engagement with banking apps. *Journal of Financial Services Marketing*, 21(1): 51–63. <https://doi.org/10.1057/fsm.2016.1>.
- Williamson, G.D., 2006. Enhanced authentication in online banking. *Journal of Economic Crime Management*, 4(2): 1–42.
- Wilson, M., 2020. The eye of providence: The symbol with a secret meaning? *BBC Culture*, 13 November. [online] Available at: <<https://www.bbc.com/culture/article/20201112-the-eye-of-providence-the-symbol-with-a-secret-meaning>> [Accessed 2 November 2020].

- Winkie, L., 2021. *Elder-Friendly Technology Is a Growing Market*. [online] Available at: <<https://www.vox.com/the-goods/22689802/elder-friendly-technology-grandpad-jitterbug-old-people-tablets>> [Accessed 8 October 2021].
- Yazdanifard, R., Wanyusoff, W.F., Behora, A.C. and Sade, A.B., 2011. Electronic banking fraud: The need to enhance security and customer trust in online banking. *Advances in Information Sciences and Service Sciences*, 3(10): 505–509. <https://doi.org/10.4156/AISS.vol3.issue10.61>.
- Yevseyeva, I., Turland, J., Morisset, C., Coventry, L., Groß, T., Laing, C. and Van Moorsel, A., 2015. Addressing consumerization of it risks with nudging. *International Journal of Information Systems and Project Management*, 3(3): 5–22. <https://doi.org/10.12821/ijispm030301>.
- Zhang, B. and Xu, H., 2016. Privacy nudges for mobile applications: Effects on the creepiness emotion and privacy attitudes. *Proceedings of the ACM Conference on Computer Supported Cooperative Work (CSCW)*, 27: 1676–1690. <https://doi.org/10.1145/2818048.2820073>.
- Zhang-Kennedy, L., Chiasson, S. and Van Oorschot, P., 2016. *Revisiting Password Rules: Facilitating Human Management of Passwords*. Paper presented at the 2016 APWG Symposium on Electronic Crime Research. [online] Available at: <<https://uwspace.uwaterloo.ca/bitstream/handle/10012/18096/Revisiting%20Password%20Rules%20-%20Facilitating%20Human%20Management%20of%20Passwords.pdf;jsessionid=37FE7347FF05FE20CF4BCA5517C499F0?sequence=2>> [Accessed 2 November 2020].
- Zhong, C.B., Bohns, V. and Gino, F., 2010. Good lamps are the best police: Darkness increases dishonesty and self-interested behavior. *Psychological Science*, 21(3): 311–314. <https://doi.org/10.1177/0956797609360754>.
- Zulkipli, N.H.N., Rashid, N.A., Zolkeplay, A.F. and Buja, A.G., 2021. Synthesizing cybersecurity issues and challenges for the elderly. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(5): 1775–1781. <https://doi.org/10.17762/turcomat.v12i5.2180>.

APPENDICES

APPENDIX A: NUDGE MECHANISMS AND COM-B FACTOR MAPPING

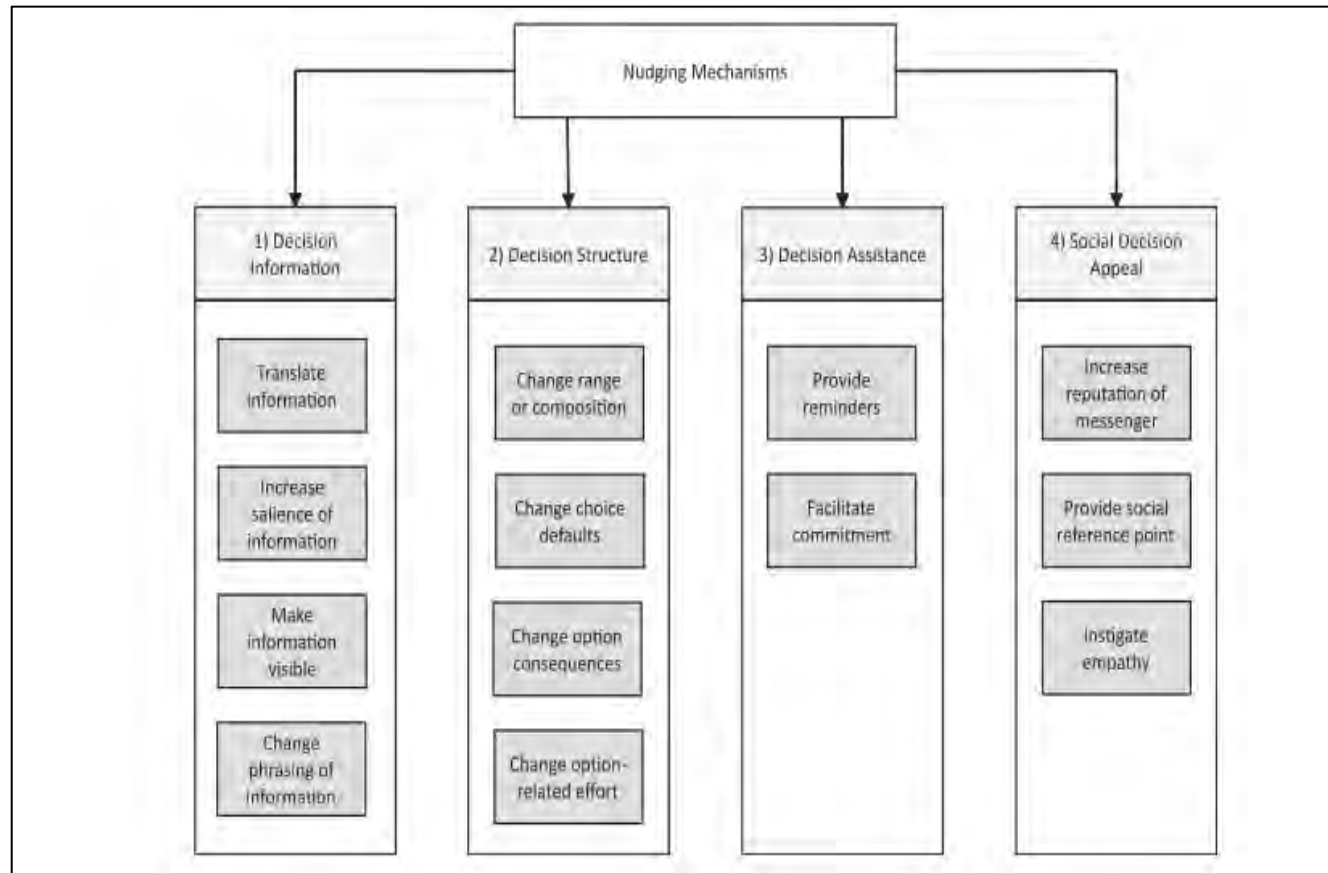


Figure A1: Taxonomy of nudging mechanisms

Source: Jesse and Jannach (2021)

The four main categories of nudging mechanisms are decision information, decision structure, decision assistance, and social decision appeal (Jesse and Jannach, 2021). Social decision appeal was the category added beyond the original taxonomy by Münscher, Vetter and Scheuerle (2016). While other studies also examined similar nudging mechanisms, Jesse and Jannach (2021) provide the most comprehensive summary of the nudging mechanisms.

Decision Information

Decision information refers to a category of nudges that impact what information is presented to the nudgee and how it is presented (Jesse and Jannach, 2021). The general goal with this category of nudges is to reduce the cognitive effort the user needs to understand what they are doing on a website. This category of nudges can be broken down into four subcategories: translate, salience, visibility, and phrasing. Figure A2 provides an overview of this category and all its nudging mechanisms (decision information also being the category with the most nudging mechanisms among the four). By making it easier for the nudgee or user of the website to understand the information presented on the website, most information falls under the psychological capability factor of the COM-B model.

| 1) Decision Information | | | | |
|---|--|---|---|---|
| Translate information | Increase salience of information | Make information visible | | Phrasing of information |
| <ul style="list-style-type: none"> • Decrease vagueness and ambiguity • Explicitly mapping • Simplification • Understanding mapping | <ul style="list-style-type: none"> • Attracting/Reducing attention • Hiding information • Increase salience of attribute • Increase salience of incentives • Using visuals to deceive • Using visuals to increase salience | <ul style="list-style-type: none"> • Checklist • Customized information • Disclosure • Give comparative information • Informing • Make external information visible | <ul style="list-style-type: none"> • Providing an explanation • Providing feedback • Providing multiple viewpoints • Reduce the distance • Suggesting alternatives • Visible goals • Warning | <ul style="list-style-type: none"> • Anchoring and adjusting • Attentional collapse • Availability • Biasing the memory of experiences • Decoy effect • Endowment effect • Framing • Hyperbolic discounting • Image motivation • Limited time window • Loss aversion • Make resources scarce • Mental accounting • Optimism and overconfidence • Placebos • Priming • Representativeness • Spotlight effect • Temptation |

Figure A2: Decision information nudges

Source: Jesse and Jannach (2021)

Translate Information

The translate information subcategory of nudges focuses on summarising complex and/or large amounts of information into something easy to grasp. This helps users to understand the impact of the actions they can take with the online banking account. ✖

- **Decreasing vagueness and ambiguity:** As implied by the name, making it more straightforward and less up to interpretation helps the user to understand (Jesse and Jannach, 2021). It also helps to avoid confusion and misinterpretation about the various options on the website; thus, using a plain or common language with no alternate meaning on the website.
- **Explicitly mapping:** When users are presented with multiple options, it is useful to explain them in terms of their cost/benefit (Thaler and Sunstein, 2008; Jesse and Jannach, 2021). In the context of online banking, this would mean explaining the potential financial impact of the options available on the website.
- **Simplification:** Reducing the cognitive effort needed to understand the decision by making it shorter or more straightforward (Ly, Zhao and Soman, 2013; Sunstein, 2014; Acquisti et al., 2017; Jesse and Jannach, 2021). In other words, reducing the number of steps and information the user needs to process to complete tasks on the site.
- **Understanding mapping:** Use of familiar analogies or visual aides to explain complex or unfamiliar concepts (Jesse and Jannach, 2021). On an online banking website, icons are used to visually give users an idea of what the various options do.

All four of these nudges fall under the psychological capability factor of the COM-B model as they help the user to understand the information presented on the site better. As a result, it would allow them to use the website better

Increase Salience of Information

This subcategory of nudging mechanisms deals with making certain information or options more prominent on a user interface (UI) to draw the user's attention. These options are more likely to stay at the forefront of the users' thoughts as they navigate the website (Jesse and Jannach, 2021).

- **Attracting/reducing attention:** Using some form of highlighting to draw the user's focus towards the more important aspects of the page/UI (Jesse and

Jannach, 2021). An online banking website can therefore highlight an option such as “Manage accounts”, “Transfers”, or “Payments”.

- **Hiding information:** Make the less desirable options harder to see (Jesse and Jannach, 2021). An example of this on an online banking website would require the user to scroll down to see the option to lock their online banking account, while options such as transfers and payments are immediately visible when the page loads.
- **Increase the salience of the attribute:** Using UI attributes such as weight, price, or colour to make a choice or aspect of the page/UI stand out more (Jesse and Jannach, 2021).
- **Increase the salience of incentives:** Make the incentives for the option(s) more visible to users to help pique their interest more (Jesse and Jannach, 2021). For example, the bank can prominently lower transaction costs and interest rates to get online banking users to sign up for a new credit card online.
- **Using visuals to deceive:** Using things like optical illusions to make certain aspects of the page/UI appear more salient than they actually are (Caraban et al., 2019; Jesse and Jannach, 2021). Renaud et al. (2017) and Thaler and Sunstein (2008) bring up the example of Schiphol Airport in Amsterdam, where images of common houseflies were painted on the urinals in male bathrooms. This reduced the spillage around the urinals by motivating (tricking) people using the urinals to aim for the fly.
- **Using visuals to increase salience:** Using visual effects like colours, pictures, signs, or fonts (UI elements) to make information more salient (Jesse and Jannach, 2021). It is similar to the previously mentioned mechanism, namely “increase salience of attribute”. In general, imagery can make one option look more or less attractive to others.

For the most part, this subcategory of nudges is linked to psychological capability as it makes useful information more visible to users; thus helping them use the site better. The exception is deceptive visualisations, as images have a positive effect on motivation, according to Caraban et al. (2019).

Make Information Visible

This subcategory focuses on providing pertinent information to the user to help them navigate the website/UI and decide which option to take.

- **Checklist:** The use of checklists to help users track their progress through different use cases or forms (Jesse and Jannach, 2021). The checklist acts as a visual guide and form of feedback on the users' completed steps and remaining steps before the task is complete.
- **Customised information:** Reduce the cognitive load on the user by showing them only the information they need (Jesse and Jannach, 2021). For example, if the user is performing a money transfer, only details like recipient bank, branch code, account number, and the amount are requested by the website.
- **Disclosure:** Reveal the relevant information about a particular option (Sunstein, 2016; Jesse and Jannach, 2021); for example, the transaction and other charges associated with opening a new current account.
- **Give comparative information:** Give users information that is “comparative to the point of view” (Jesse and Jannach, 2021). Not too applicable to an online banking context, but an example would be the “other users also viewed” notices provided when shopping online.
- **Informing:** Simply giving the user additional information that may be helpful to their current task (Jesse and Jannach, 2021). This is similar to the behavioural intervention of notice described by Calo (2014).
- **Make external information visible:** Give the user additional information created by a third party (Jesse and Jannach, 2021).
- **Providing an explanation:** More information about the current situation/step the user is in at the moment (Jesse and Jannach, 2021). An example would be to use tooltips to provide helpful hints about the options available to the user.
- **Providing feedback:** Helps users understand if they are “on the right track” or making mistakes (Thaler and Sunstein, 2008; Jesse and Jannach, 2021). The online banking website should clarify when the user has succeeded in performing their desired action or made an error.
- **Providing multiple viewpoints:** Helps create an unbiased overview of a particular decision to help users with the problem at hand (Jesse and Jannach,

2021). Not too applicable to the online banking website context. An example would be allowing users to read other customer reviews while shopping online.

- **Reduce the distance:** If a problem or situation is too far off, users will feel little to no urgency to act upon the potential threat. Presenting users with similar situations can help reduce the psychological distance (Jesse and Jannach, 2021). In online banking, this could mean alerts about recent incidents of security breaches or scams at another local bank. This could encourage users to better secure their accounts, as the threats to their funds no longer seem so far off.
- **Suggesting alternatives:** Give users options they may not have considered before (Jesse and Jannach, 2021). With an online banking website, this could involve suggesting other banking services the customer could use to try to accomplish their goal.
- **Visible goals:** Give users a way to gauge their progress towards a certain goal(s) (Jesse and Jannach, 2021), similar to using a checklist.
- **Warning:** Use visual aides to warn the user about the main problem/issue (Jesse and Jannach, 2021). In the case of online banking, warnings or confirmation dialogues can be provided when the user is about to perform a difficult-to-reverse action, such as transferring funds to another bank account.

Most of the nudges in this subcategory also fall under psychological capability due to their focus on information. Exceptions are checklist, multiple viewpoints, reduce distance, and visible goals. Most of these exceptions fall under the reflective motivation factor of the COM-B model (Caraban et al., 2019). Checklist and visible goals show users what they have accomplished thus far, and what remains could motivate them to complete the process. Multiple viewpoints fall under motivation because they allow users to slow down, consider other people's opinions, and create an unbiased view. Reduce the distance makes potential problems "hit closer to home" and can motivate users to give them more time and consideration.

Phrasing of Information

This subcategory of nudges focuses on changing how information is presented to the user to influence their behaviour.

- **Anchoring and adjustment:** Exploiting the human bias of anchoring and adjustment to help nudge users towards the desired option; in other words, providing an initial point of reference for users to use when they encounter new/unfamiliar concepts on the online banking website (Thaler and Sunstein, 2008; Jesse and Jannach, 2021; Luguri and Strahilevitz, 2021).
- **Attentional collapse:** Perception of a UI is affected by what draws a user's attention. Users can miss certain information that is also present on the page when something else is more prominent and draws their attention (Jesse and Jannach, 2021). For example, suppose an online banking website has a small "out of the way" notification regarding the cookies collected by the website. In that case, some users can miss this notification and not change the privacy settings.
- **Availability:** Users are more likely to believe that an event could occur the easier it comes to mind or can be remembered (Jesse and Jannach, 2021). Similar to the reducing the distance mechanism mentioned with the make information visible subsection nudge related to a recent report of a local bank's security incident, it can make users more cautious when securing their online banking account.
- **Biasing the memory of experiences:** Tweaking the ending of an event can alter how that event will be remembered (Jesse and Jannach, 2021). For example, when a user creates a new recipient, making the progress bar move faster can make them remember the process as being quicker than it actually was.
- **Decoy effect:** Adding additional options that are worse (lower in value) to help make the desired option seem better by comparison (Caraban et al., 2019; Jesse and Jannach, 2021). An example would be opening a new account; a current account can have transaction charges of 1%, while decoy options such as "special current account" and "investment account" can have transaction charges of 12% and 15 % respectively.

- **Endowment effect:** Human tendency to overemphasize the value of objects we own. People are more likely to keep an item if they already have a similar item, rather than if they need to put in the effort to acquire something they do not already have (Caraban et al., 2019; Jesse and Jannach, 2021). For example, when trying to open a new savings account online, the user's average monthly savings balance can be shown. The potential savings plan they could choose can be compared using the estimated savings balance and highlighting the difference with their current savings balance. By phrasing it this way, the user is more likely to select the savings account that improves their savings balance.
- **Framing:** Whether the information presented to the user is phrased in a way that puts it in a negative or positive light can affect the user's final decision (Mirsch, Lehrer and Jung, 2017; Jesse and Jannach, 2021). The previous example of opening a savings account online can also apply here. Describing opening a new savings account as a decrease in average monthly bank balance can prevent people from saving. Alternatively, describing opening a savings account as a long-term investment that generates some interest can encourage people to open a new account.
- **Hyperbolic discounting:** People can decide to take certain options when the consequences seem much further away and have less of an immediate impact (Mirsch et al., 2017; Schaer and Stanoevska-Slabeva, 2019; Jesse and Jannach, 2021). For example, people can decide to buy a new television on credit rather than pay the full cash price now, even though, in the long run, it may end up costing them much more than the cash price.
- **Image motivation:** People love to accept the credit when things go well, but they deflect to other people/causes when things "go sideways" (Jesse and Jannach, 2021). For example, while using online banking, if a customer makes a typo and transfers funds to the wrong recipient, they could blame the website for not providing a confirmation/summary page to confirm the recipient's details.
- **Limited time window:** The (false) impression of being scarce or exclusive can be created when people believe an option will expire after some time (Jesse and Jannach, 2021). Not too applicable to the online banking context, but an example could be a limited-time discount while shopping online.

- **Loss aversion:** Phrasing something in terms of the negative loss has a greater impact than phrasing it as the equivalent positive gain (Jesse and Jannach, 2021). The savings account example used for the framing and endowment effect can also work here. People are less likely to open a savings account if it is phrased as \$100 less disposable income rather than \$100 more in savings.
- **Make resources scarce:** Making an option or resource seem limited in some way makes users more likely to choose it (Jesse and Jannach, 2021). Similar to the “limited time window” described earlier, options that seem rarer or limited are often more desirable to users.
- **Mental accounting:** Users mentally sort their payments/transactions into certain groups, although this may not accurately represent what is happening to their funds (Jesse and Jannach, 2021). For example, allowing users to group certain recipients under the option of a “Bills” category can help online banking clients manage their monthly expenses.
- **Optimism and overconfidence:** Users may have a habit of overestimating their capabilities and the potential rewards from certain options/decisions (Jesse and Jannach, 2021). An example of a nudge aimed at combatting this would be the example from the reducing the distance mechanism. A security incident at another local bank would likely make the user less lax regarding securing their account.
- **Placebos:** Changing user behaviour by providing an additional option or UI element that, in actuality, does little to nothing, but that the user may perceive to have additional benefits (Caraban et al., 2019; Jesse and Jannach, 2021).
- **Priming:** Exposing a user to a certain stimulus beforehand can influence their decision/behaviour as the user may remember it subliminally (Caraban et al., 2019; Jesse and Jannach, 2021). For example, briefly seeing an advertisement for a new candy bar while driving to work earlier in the day can result in them buying a snack at the till when they pass by the grocery store on the way back from work.
- **Representativeness:** A heuristic/bias that causes people to estimate the chances of an event or infer someone else’s characteristics based on their mental model rather than accurate information (Schaer and Stanoevska-

Slabeva, 2019; Cherry, 2021; Jesse and Jannach, 2021). In other words, they may be stereotyping.

- **Spotlight effect:** Users overestimate how important their actions are or how much others may care or are observing them (Thaler and Sunstein, 2008; Jesse and Jannach, 2021). An example of a nudge exploiting this would be a notice regarding transaction monitoring. If the online banking website warns the user that the bank verifies transactions every hour, it could dissuade unauthorised users from committing fraud. The unauthorised user could believe that any fraudulent transactions they carry out will be detected by a bank employee monitoring that specific account.
- **Temptation:** Users prefer options that provide a more immediate reward than delayed gratification (Jesse and Jannach, 2021).

The focus on information also makes this subcategory of nudging mechanisms mostly fall under the psychological capability factor of the COM-B model. According to Caraban et al. (2019), placebos, decoys, priming, and scarcity are exceptions in this subcategory and would likely fall under the motivation factor. Priming, for the most part, would fall under the subfactor of automatic motivation, as the stimulus the user is exposed to can easily be missed. For the most part, placebos, decoys, and scarcity would fall under reflective motivation as the users consider their options or think about seizing a “limited” opportunity in the case of scarcity.

Change Defaults

This subcategory focuses on using the default option as a subtle nudge towards the desired option by using it as the default choice. When people have difficulty deciding, they may often resort to the default choice. These nudges often exploit the status quo bias: the reluctance to change existing or familiar circumstances and try something new (Thaler and Sunstein, 2008; Caraban et al., 2019).

- **Automatic enrolment:** Users need to make an active choice not to be enrolled or opt out (Jesse and Jannach, 2021). For example, if a bank client signed up for online banking, two-factor authentication (2FA) via email can be enabled by default, and the user would have to change their settings once logged in to remove it.

- **Enhancing or influencing active choosing:** Prompt to actively choose an option combined with other nudges to guide the user's decision towards a certain option (Jesse and Jannach, 2021).
- **Prompted choice:** Prompts force users to make an active choice (Jesse and Jannach, 2021). An example applicable here could be a confirmation dialogue box where the user must click "yes" to perform a transfer or make changes to their account.
- **Setting defaults:** When multiple options are available, users often tend to maintain the status quo and leave the pre-selected default on (Jesse and Jannach, 2021). The choice architect can take advantage of this.
- **Simplifying active choosing:** Increases the chances of users considering their decision and potential consequences (Jesse and Jannach, 2021). Making it less complicated to decide can help reduce the cognitive load on the user.

The default nudges generally fall under the capability factor of the COM-B model as they all aim to simplify the decision-making process for the user, although being forced to make an active decision does mean that a few of these mechanisms can overlap with reflective motivation.

Decision Structure

Decision structure refers to a category of nudges that focuses on the arrangement of options available to the nudgee (Jesse and Jannach, 2021). This category of nudges can be broken down into four subcategories: defaults, option-related efforts, range/composition of options, and option consequences. Figure A3 summarises all the nudges in this category.

| 2) Decision Structure | | | |
|--|--|--|---|
| Change choice defaults | Change option-related effort | Change range or composition of options | Change option consequences |
| <ul style="list-style-type: none"> • Automatic enrollment • Enhancing or influencing active choosing • Prompted choice • Setting defaults • Simplifying active choosing | <ul style="list-style-type: none"> • Change ease and convenience • Change financial effort • Change physical effort • Create friction • Navigability of contexts • Reduce paperwork • Speed bumps • Throttle mindless activity | <ul style="list-style-type: none"> • Change scale • Decision staging • Order effects • Partition of options or categories • Structure complex choice • Structure of evaluation | <ul style="list-style-type: none"> • Change social consequences • Connect decision to benefit or cost • Micro-Incentives |

Figure A3: Decision structure nudges

Source: Jesse and Jannach (2021)

Change Option-Related Effort

This subcategory focuses on creating an imbalance of effort required between the various options. In other words, make the more desirable options easier to take, while the less desirable options are harder for the nudgee to choose.

- **Change ease and convenience:** Alter the options available to make the desirable choice more accessible or convenient than others (Jesse and Jannach, 2021). The more convenient option is more likely to be chosen by the nudgee, who wants as little hassle as possible.
- **Change financial effort:** The choice architect can alter the financial effort between various options available to the nudgee (Hummel and Maedche, 2019; Jesse and Jannach, 2021). An easy example would be retail shopping. To pay for a good, the choice architect can offer the option for full cash payment or much smaller monthly payments on credit. With the latter, the customer can get the good in question, but in the long term, they may pay more than the cash price.
- **Change physical effort:** Make undesirable options physically harder to choose or perform (Jesse and Jannach, 2021). For example, reminders about how online banking can be done in the comfort of their own home. This can nudge the bank's clients to use online banking more rather than visiting their closest branch.
- **Create friction:** Nudges that focus on minimising intrusiveness in the decision-making process while still being able to alter behaviour (Caraban et al., 2019; Jesse and Jannach, 2021). Intrusiveness refers to the need to divert all one's attention to a single activity and decide. For example, when about to take the elevator, the LED screen showing the floor numbers can quickly display (scroll through) the message "It's healthier for you, and probably quicker to take the stairs".
- **Navigability of contexts:** Make it easy to switch or navigate various contexts (Jesse and Jannach, 2021). In other words, designing a website that is easy to navigate and provides helpful tips for the users.

- **Reduce paperwork:** Reduce the amount of paperwork necessary for certain tasks (Jesse and Jannach, 2021). Banks already employ this nudge; the lack of paperwork is often used to market online banking to their clients.
- **Speed bumps:** Provide methodical “speed bumps” to get the user to slow down and contemplate as they go through a task/process (Jesse and Jannach, 2021). For example, providing a loading screen between a transaction and a confirmation page. By having users wait rather than it be instantaneous to do a transfer or make account changes, they can stop and think and potentially cancel.
- **Throttle mindless activity:** Reduce the time users can spend on “autopilot” when performing certain tasks or give them ways to recover from making certain mistakes (Jesse and Jannach, 2021). Something like form validation and confirmation dialogues can apply here. By having the user double-check the details they enter on a form, they are more likely to correct minor, easy-to-avoid mistakes such as typos.

Most of the nudges in this category fall under the capability factor of the COM-B model. In the context of an online banking website, these nudges would most likely fall under psychological capability, but under different contexts, they could fall under physical capability and physical opportunity subfactors as well. For example, placing healthy snacks at eye level at a food stand and making less healthy alternatives harder to see and reach. According to Caraban et al. (2019), friction is an exception as it creates reminders about alternatives and could thus fall under reflective motivation and physical opportunity.

Change Range or Composition of Options

This subcategory, as the name implies, focuses on the options presented to the user and how they are arranged or displayed to them.

- **Change scale:** By expressing numerical information in a way that makes it appear larger, the differences between options appear greater than they actually are, e.g., \$1 and \$2 vs 100 and 200 cents; thus, increasing the weight/significance of this information to the user (Johnson et al., 2012; Jesse and Jannach, 2021).

- **Decision staging:** Breaking down complex decisions into smaller, more manageable steps that are grouped appropriately (Jesse and Jannach, 2021). This allows users to complete all the necessary steps in a systematic way that is easy to follow; for example, the different steps when completing a form.
- **Order effects:** The order in which the average user notices things on a page or UI is important. What they easily/first pick up on is perceived as more important (Caraban et al., 2019; Jesse and Jannach, 2021). As a result, how the options are ordered can impact the decision of the nudgee. Turland et al. (2015) employed ordering as part of their nudging study on wireless networks. Placing the more secure networks at the top helped users to avoid selecting unsecured or open networks.
- **Partition of options/categories:** How things on the page itself are grouped/categorised. Separating and putting desired and undesirable options in their own groups can help nudge users towards the more desirable choice (Johnson et al., 2012; Jesse and Jannach, 2021).
- **Structure complex choices:** Make complex decisions easier by breaking them down into smaller steps, e.g., guiding users through a process (Jesse and Jannach, 2021). Similar to the example from decision staging, the user is guided through a process to ensure they do not miss or omit anything important.
- **Structure of evaluation:** How the final results are presented can influence the user's behaviour. Displaying a single item at a time can result in a different outcome than displaying all items at once (Jesse and Jannach, 2021).

The nudges under this subcategory would primarily fall under capability. They could also touch upon motivation and opportunity to a lesser extent, although opportunity again would be more context dependent than the other factors. In the context of online banking, arranging these nudges would affect how the various options and functionality of the site are displayed to the user. This could make it easier for the user to understand how to use the site as everything is grouped/arranged in a more intuitive way. Thus, they mostly fall under psychological capability and, to a lesser extent, physical capability, as visibility and positioning on the page can make certain options easier or harder to see and click (choose).

Change Option Consequences

This subcategory of nudges focuses on altering the protentional consequences of each of the choices available to the user. The goal is to tweak the consequences in such a way that the choice architect's more desirable option seems more appealing to the nudgee.

- **Change social consequences:** Make it easy to link actions/options to certain social consequences (Jesse and Jannach, 2021); for example, friends will see the option chosen.
- **Connect decision to benefit/cost:** Behaviour/choice can be influenced by making the link between benefits/costs of each option apparent (Münscher et al., 2016; Jesse and Jannach, 2021). For example, confirmation dialogue for completing a transfer or payment can include the actual amount being transferred, potential bank charges, and the new balance.
- **Micro-incentives:** Changes to the consequences that are relatively insignificant to the final decision (Hummel and Maedche, 2019; Jesse and Jannach, 2021). For example, a small incentive like continued purchases from the same supermarket will reward customers with a few loyalty points for each purchase.

The nudges under this subcategory would fall under the reflective motivation subfactor. The additional information about the potential benefits or costs for each potential action would likely make the user or nudgee consider their options more. Social consequences, however, would also overlap with the social opportunity subfactor.

Decision Assistance

Decision assistance refers to a category of information that provides decision support to the nudgee (Jesse and Jannach, 2021). This category of nudges can be broken down into two subcategories: reminders and commitment. Figure A4 provides an overview of the nudging mechanisms under this category.

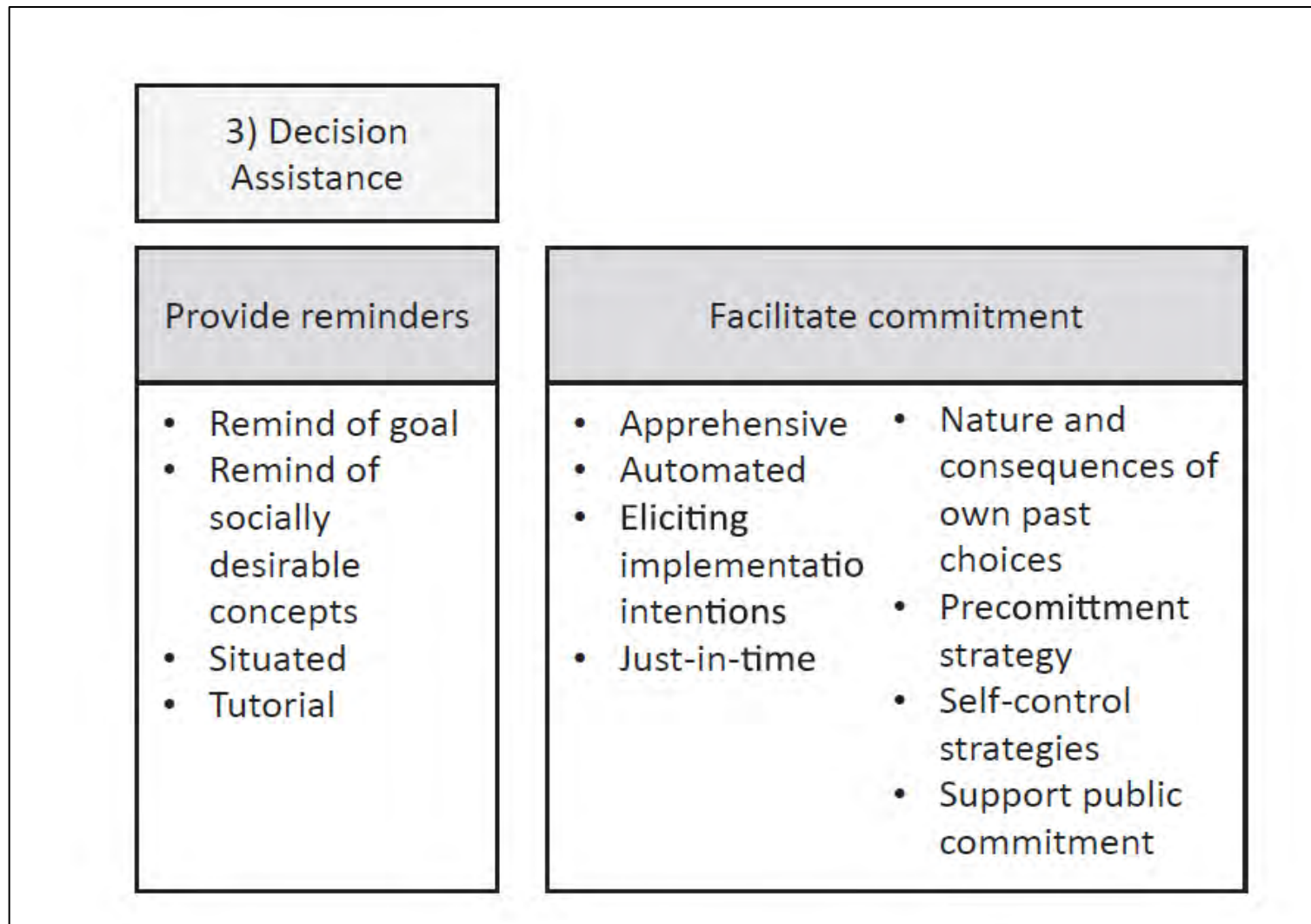


Figure A4: Decision assistance nudges

Source: Jesse and Jannach (2021)

Provide Reminders

This subcategory focuses on reminding users about their final goals and the potential benefit of completing a long process. The reminders themselves can also be used to promote the more desirable options.

- **Remind of goals:** Inform the user again about what will happen at the end of the process to remind them why they should complete it (Mongin and Cozic, 2014; Münscher et al., 2016; Caraban et al., 2019; Jesse and Jannach, 2021). For example, a reminder to complete online banking account setup by completing additional security options to help secure their account.
- **Remind of socially desirable concepts:** Make certain social norms/values more apparent at the moment of the decision (Münscher et al., 2016; Jesse and Jannach, 2021). For example, a reminder to set up retirement savings account popping up after logging in to online banking.
- **Situated:** Providing useful hints and reminders for the specific task the user is currently performing (Jesse and Jannach, 2021). For example, after conducting multiple payments to a recipient, an alert can pop up, offering to show the user how to set up scheduled payments or debit orders.
- **Tutorial:** Teach users how to perform specific processes/steps so that they can later do it themselves (Jesse and Jannach, 2021). The online banking website can employ a Frequently Asked Questions page or concise video tutorials for certain features on the site to help guide their clients.

Among this subcategory of nudges, situated and tutorial would fall under the capability factor of the COM-B model. These nudges are meant to help provide some form of assistance to the user. The remaining two reminder nudges would fall under the reflective motivation factor.

Facilitate Commitment

Nudges that focus on encouraging users to engage with their preferred option and stick with it until the end due to promises or pledges made to themselves or others. This is a subcategory of decision assistance nudges.

- **Apprehensive:** Providing the user with multiple ways to achieve the same outcome (Jesse and Jannach, 2021); for example, to help their clients manage

their bills, banks can encourage them to set up scheduled payments or debit orders.

- **Automated:** Minimises or removes the need for user input for specific actions (Jesse and Jannach, 2021). The previous debit order example can also apply here since once it is set up, the payment is repeated automatically every month around the same date.
- **Elicit implementation intentions:** Users are more likely to finish their current task/action if someone asks them about their final goal. For example, when making another payment to a recipient, a pop-up can ask, “Do you wish to set up scheduled payments to this recipient?”
- **Just-in-time:** User recommendations pop up only when appropriate to their current activity/decision (Jesse and Jannach, 2021). Similar to the situated nudging mechanism form of “provide reminders” (see Section 4.3.3.1), a nudge like this can be done by offering a link to a help page for the user’s current task, i.e., “How to add new recipients?” or “How to set up debit orders?”
- **Nature and consequences of own past choices:** With historical data, it is possible to explain previous choices/actions and why they should be repeated (Sunstein, 2014; Jesse and Jannach, 2021). The debit order example can apply here too; after a set number of regular payments to the same recipient, a pop-up suggesting debit orders or scheduled transfers can be displayed to the user.
- **Precommitment strategy:** Lets users define or plan how to complete specific objectives/tasks (Sunstein, 2014; Jesse and Jannach, 2021); for example, give online banking users the option to set up their savings plans and send them reminders about their pre-set savings goals later.
- **Self-control strategy:** Supports users so they do not fall victim to their own weaknesses, e.g., heuristics and biases (Jesse and Jannach, 2021). The savings plan example can also apply here. Appropriate reminders about their savings goals/targets could help clients to manage their spending.
- **Support public commitment:** Promises/pledges made publicly can increase the likelihood they will follow through (Münscher et al., 2016; Jesse and Jannach, 2021). Not applicable to the online banking context, but making a public announcement about a sizeable charitable donation can encourage an individual to pay the funds they pledged.

Most of the nudges in this subcategory would fall under reflective motivation as they focus on getting the user to slow down and consider their options, usually with some (long-term) goal in mind. Public commitment also falls under the reflective motivation subfactor, but there is some overlap with the social opportunity subfactor by using social norms to influence behaviour. Similar to tutorial and situated nudges, just-in-time would also fall under the capability factor. In the context of online banking, this would mostly be psychological capability. Apprehensive and automated nudges would also fall under capability. The former is because it gives the users various ways to use the website; the latter is due to performing certain functions for the user and reducing the effort/input needed from them.

Social Decision Appeal

Social decision appeal is the final category of nudging mechanisms that focuses on exploiting social influence and comparisons made by the nudgee (Jesse and Jannach, 2021). This category of nudges can be broken down into three subcategories: messenger reputation, social reference points, and instigating empathy. Figure A5 provides an overview of the nudges in this category.

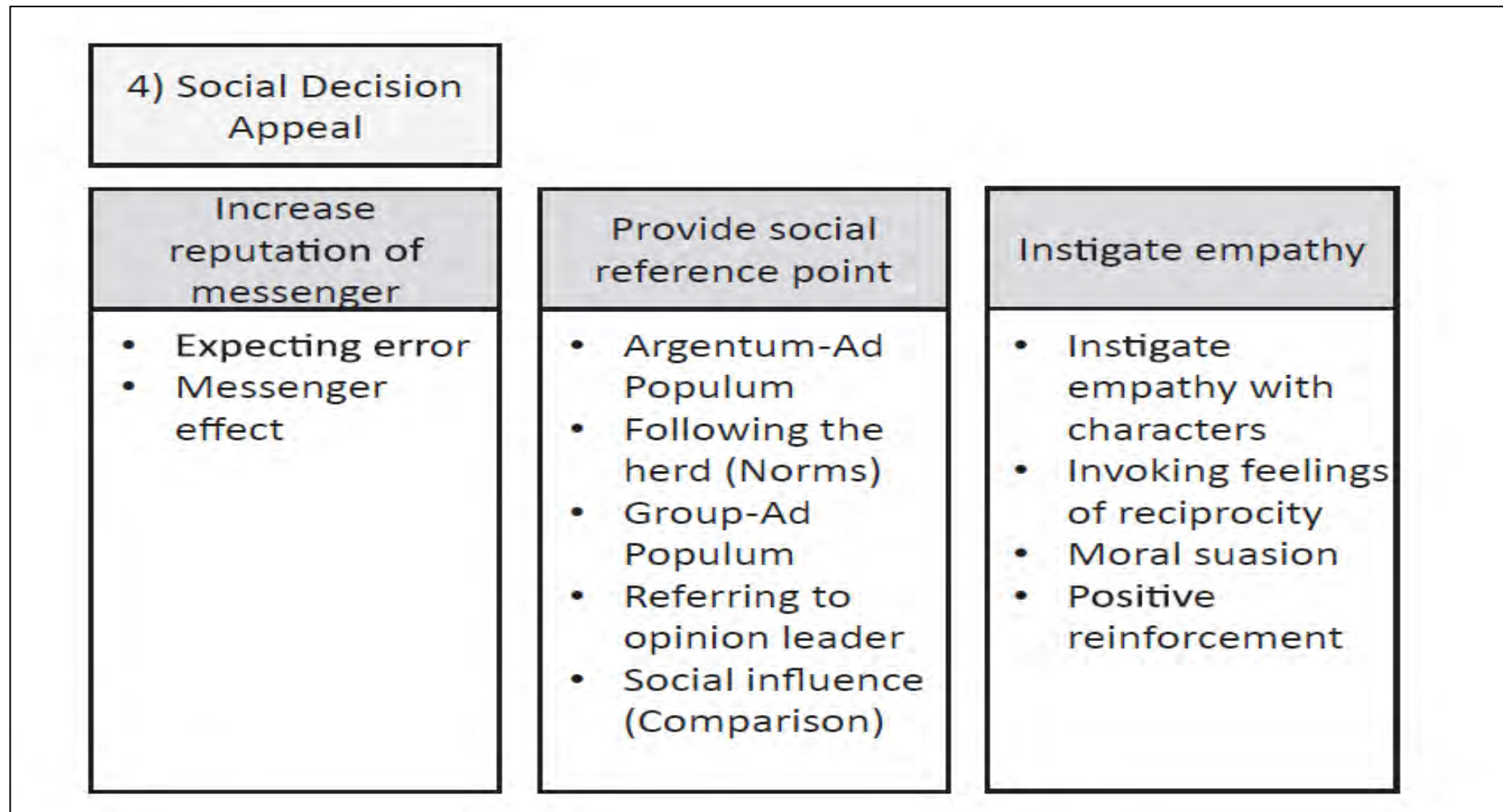


Figure A5: Social decision appeal nudges

Source: Jesse and Jannach (2021)

Increase Reputation of Messenger

This subcategory of nudges focuses on improving the reputation of the messenger; in this case, the bank and its website. The better the reputation of the messenger, the more the message they are trying to send will be taken to heart by the recipient; in this case, the user. Positive experiences can encourage a bank's clients to use their bank's online service more often.

- **Expecting error:** By being more forgiving when users make mistakes, the reputation of the messenger improves (Jesse and Jannach, 2021). By designing the online banking website with the expectation of some user error in mind, it could become more user friendly. For example, when making a payment, the user can be given multiple opportunities to confirm that the recipient details they entered are correct.
- **Messenger effect:** Who or what delivers a message creates certain perceptions for a user (Jesse and Jannach, 2021). In the case of the bank and its website, it is how they choose to communicate to their customer. For example, an email with their account statement attached can seem more official or professional than a simple SMS with their balance.

As they are part of the broader social decision appeal, both these nudges naturally fall under the social opportunity subfactor. Expecting nudges, however, would also fall under the capability factor.

Provide Social Reference Point

This subcategory of nudges focuses on exploiting social norms and comparisons to encourage certain behaviours or decisions.

- ***Argumentum ad populum*:** Accepting certain beliefs or theories because most people already accept them (Jesse and Jannach, 2021). For example, the bank can market its online service by using the results of surveys that illustrate the widespread belief that online banking is secure and convenient. For example: "92% of clients surveyed agree that online banking is safe, fast and convenient".
- **Following the herd:** To avoid standing out too much, users may behave similarly to how the majority behaves (Jesse and Jannach, 2021). Not very

applicable to the online banking context but an example could be the likes and dislikes employed on social media simply because when something has a high average rating (thumbs-up/likes, etc.), users may engage with it more.

- **Group *ad populum*:** Accepting certain beliefs or theories simply because a particular group has already accepted it (Jesse and Jannach, 2021). Not applicable to the online banking context, but an example of such a nudge could be the prompts to use something like Facebook Messenger by showing your friends who are already using it; for example: “Simon, Samantha, Bob, and Fred use Messenger. Sign up today.”
- **Opinion leaders:** Using a well-known or highly respected messenger to deliver the message can influence the opinion and behaviour of users (Jesse and Jannach, 2021). For example, a hypothetical banking advertisement using a popular local celebrity to encourage potential clients to switch over to their bank.
- **Social (influence) comparison:** Allows individuals to compare themselves to others (Jesse and Jannach, 2021). An online shopping example could be the alert that other users like you also looked at these products. This nudge could keep the user browsing the online store and potentially make more purchases.

This entire subcategory of nudges would fall under the social opportunity subfactor. To some extent, they can also fall under the motivation factor; these nudges can sway users towards certain popular options.

Instigate Empathy

As implied by the name, this subcategory of nudges focuses on increasing the empathy the nudgee feels so as to encourage certain behaviours or choices (Caraban et al., 2019; Jesse and Jannach, 2021).

- **Instigate empathy with characters:** Using avatars/mascots whose state changes based on user actions can potentially influence behaviour (Caraban et al., 2019; Jesse and Jannach, 2021). For example, using an emoticon as a gauge for password strength. A frowning emoticon can be shown when the created password is weak. A sceptical emoticon could be shown for a medium-strength password. A smiling emoticon can be shown for a very strong password.

- **Invoke feelings of reciprocity:** Doing something pleasant or beneficial for the user to create an obligation to “return the favour” (Caraban et al., 2019; Jesse and Jannach, 2021).
- **Moral suasion:** A nudge that aims to increase fun or create a sense of responsibility for a task to encourage certain behaviours (Sunstein, 2016; Jesse and Jannach, 2021).
- **Positive reinforcement:** Gives the user some form of praise or positive feedback when they take desirable options/actions (Jesse and Jannach, 2021). For example, an email from their local bank welcoming and thanking the customer for switching over to their bank can also encourage users to sign up for their online banking service.

By virtue of being part of the social decision appeal category, all the nudges under this subcategory should fall under social opportunity. Still, there is a significant overlap with other factors. Instigating empathy and positive reinforcement overlap with the capability factor as they can help the user learn and understand some of the steps they could take to avoid hurting another individual and their finances. According to Caraban et al. (2019), reciprocation can also overlap with motivation.

APPENDIX B: INTERFACES AND NUDGES

Interfaces

Control

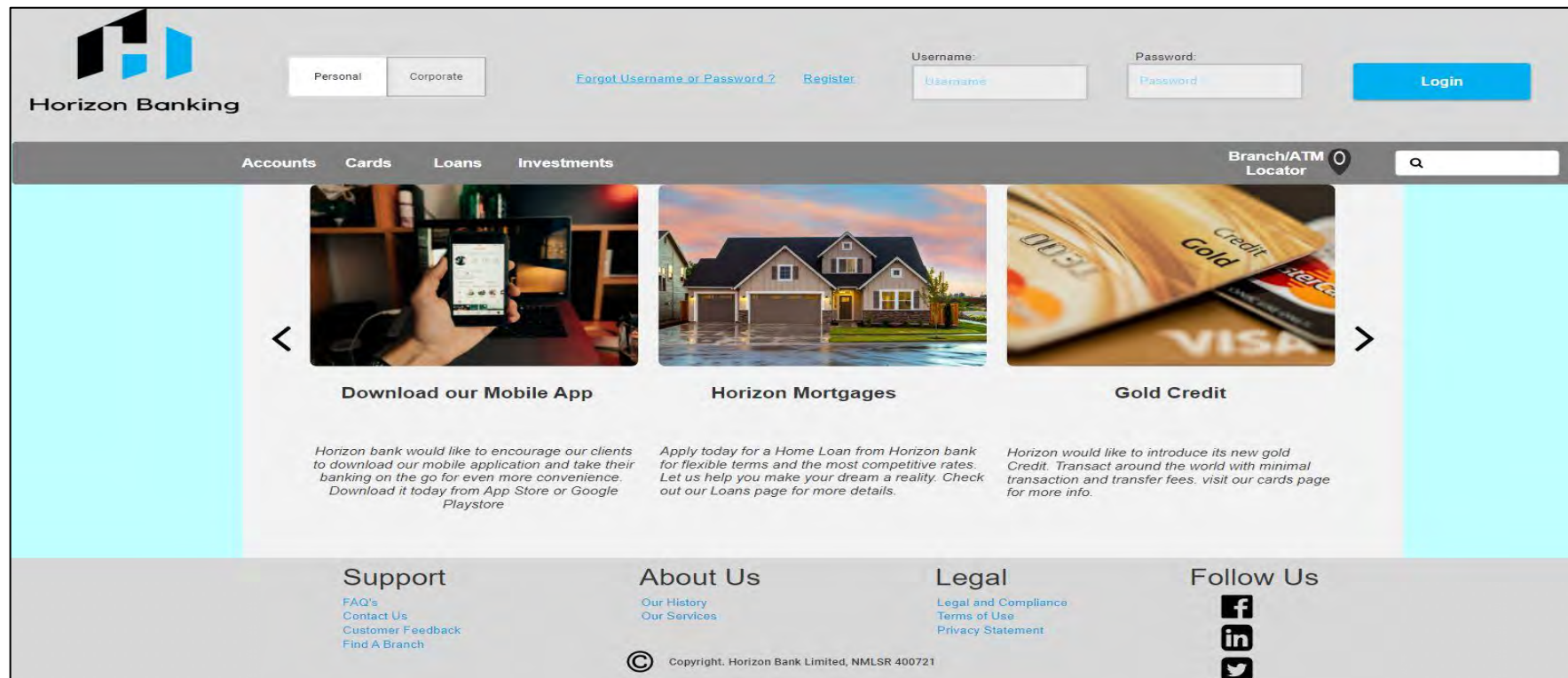



Figure B1: Control and POST-LOG homepage



V. Lawson

Logout

My Accounts

My Cards

My Loans

My Investments

Q

Summary

Transaction History

Payments

Transfers

| First Name(s) | Surname | Account type | Account Number | Balance | Available Balance |
|---------------|---------|--------------|----------------|------------|-------------------|
| Vanessa | Lawson | Checking | 6347300380 | \$ 7722.60 | \$ 7722.60 |

Today's Date 3 July 2022

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)

About Us

[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)


Follow Us





 Copyright. Horizon Bank Limited, NMLSR 400721

Figure B2: Control and PRE-LOG summary page



V. Lawson

Logout

My Accounts

My Cards

My Loans

My Investments

Summary

Transaction History

Payments

Internal Transfers

Vanessa Lawson

Account 6347300380

Account Type :

Checking Account

Today's Date 3 July 2022

| Date | Description | Ref | Amount | Balance |
|------------|------------------------------|-----------|----------|---------|
| 01-06-2022 | Opening Balance | - | - | 9782.25 |
| 02-06-2022 | Chevron Gas-POS | T1265-622 | (50.27) | 9731.98 |
| 03-06-2022 | Costco Supermarket - POS | T1265-622 | (127.47) | 9604.51 |
| 05-06-2022 | Walter & Sons Pharmacy - POS | T1265-622 | (80.00) | 9524.51 |
| 09-06-2022 | Exxon Mobil- POS | T1365-622 | (45.00) | 9479.51 |
| 10-06-2022 | Costco Supermarket-POS | T3265-622 | (85.67) | 9393.84 |
| 12-06-2022 | Subway Restaurnat- POS | T6548-622 | (30.00) | 9363.84 |
| 13-06-2022 | Cash Withdrawal | T4509-622 | (300.00) | 9063.84 |

Previous

1

2

3

Next

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)




About Us


[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)


Follow Us



Copyright. Horizon Bank Limited, NMLSR 400721

Figure B3: Control and PRE-LOG transaction history (page 1)



Horizon Banking

V. Lawson

Logout

My Accounts

My Cards

My Loans

My Investments

Summary

Transaction History

Payments

Internal Transfers

Vanessa Lawson

Account 6347300380

Today's Date 3 July 2022

Account Type : Checking Account

| Date | Description | Ref | Amount | Balance |
|------------|--------------------------|-----------|----------|---------|
| 16-06-2022 | Costco Supermarket - POS | T3532-622 | (127.47) | 8936.37 |
| 17-06-2022 | NetflixUSA | T3282-622 | (19.99) | 8916.38 |
| 17-06-2022 | Disney+US | T3698-622 | (13.99) | 8902.39 |
| 17-06-2022 | Windscribe VPN | T4128-622 | (9.00) | 8893.39 |
| 20-06-2022 | Cappellini's Restaurant | T4368-622 | (102.00) | 8791.39 |
| 21-06-2022 | Costco-Supermarket-POS | T4578-622 | (64.25) | 8727.14 |
| 22-06-2022 | ChevronGas | T5687-622 | (35.00) | 8692.14 |
| 23-06-2022 | Walter & Sons Pharmacies | T5702-622 | (105.00) | 8587.14 |

Previous

1

2

3

Next

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)




About Us


[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)


Follow Us



Copyright. Horizon Bank Limited, NMLSR 400721

Figure B4: Control and PRE-LOG transaction history (page 2)



V. Lawson

Logout

My Accounts

My Cards

My Loans

My Investments

Summary

Transaction History

Payments

Internal Transfers

Vanessa Lawson

Account 6347300380

Account Type :

Checking Account

Today's Date 3 July 2022

| Date | Description | Ref | Amount | Balance |
|------------|----------------------|-----------|----------|---------|
| 25-06-2022 | Axis Insurance | T5421-622 | (240.00) | 8347.14 |
| 25-06-2022 | Healthpoint-Gym | T5693-622 | (80.00) | 8267.14 |
| 25-06-2022 | Blueline-energy | T5639-622 | (284.54) | 7982.60 |
| 26-06-2022 | City-Rates | T4654-622 | (60.00) | 7922.60 |
| 27-06-2022 | Withdrawal | T4325-622 | (200.00) | 7722.60 |
| 30-06-2022 | Closing Balance June | | | 7722.60 |
| 01-07-2022 | Opening Balance July | | | 7722.60 |

Previous

1

2

3

Next

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)




About Us


[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)


Follow Us



Copyright, Horizon Bank Limited, NMLSR 400721

Figure B5: Control and PRE-LOG transaction history (page 3)



V. Lawson

Logout

My Accounts

My Cards

My Loans

My Investments

Q

Summary

Transaction History

Payments

Internal Transfers

Add Recipient

+

| Recipient Name | Bank | Account Num | My Ref | Last Paid |
|---------------------|-----------------|--------------|--------------|------------------|
| Samuel Lawson | Bank Of America | 263956958524 | Sam | 25 May 2022 |
| Craybar Mechanics | Capital One | 123565849875 | CarService | 13 Febraury 2022 |
| Axis Insurance | Capital One | 123669854562 | Insurer | 25 June 2022 |
| Healthpoint-Gym | Bank of America | 236945699525 | GymSubs | 25 June 2022 |
| Blueline Energy INC | Wells Fargo | 265898681524 | ElectricBill | 25 June 2022 |
| BoB Parr | Bank of America | 123213132 | Bobby Par | - |
| - | - | - | - | - |

Pay

Pay

Pay

Pay

Pay

Pay

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)

About Us

[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)

Follow Us






©

Copyright. Horizon Bank Limited, NMLSR 400721

Figure B6: Control and PRE-LOG payments page


Horizon Banking

V. Lawson

Logout

My AccountsMy CardsMy LoansMy Investments

Q

Summary

Transaction History

Payments

Internal Transfers

Default Payment Account

Account

Checking Account- 6347300380

Recipient Details

Recipient Name

Bank

Choose Bank

Account Number

My Reference

Proof of Payment

Email Address

CANCEL

ADD Recipient

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)

About Us

[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)


Follow Us





© Copyright: Horizon Bank Limited, NMLSR 400721

Figure B7: Control and PRE-LOG add recipients form



V. Lawson

Logout

My Accounts

My Cards

My Loans

My Investments

Summary

Transaction History

Payments

Internal Transfers

Make Payment to BoB Parr

Select Account

Checking Account- 6347300380

Amount

Pay And Clear Now

Select one

☐ Yes

☒ No

Cancel

Make Payment

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)




About Us

[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)

Follow Us

© Copyright. Horizon Bank Limited, NMLSR 400721

Figure B8: Control and PRE-LOG pay recipient page

186

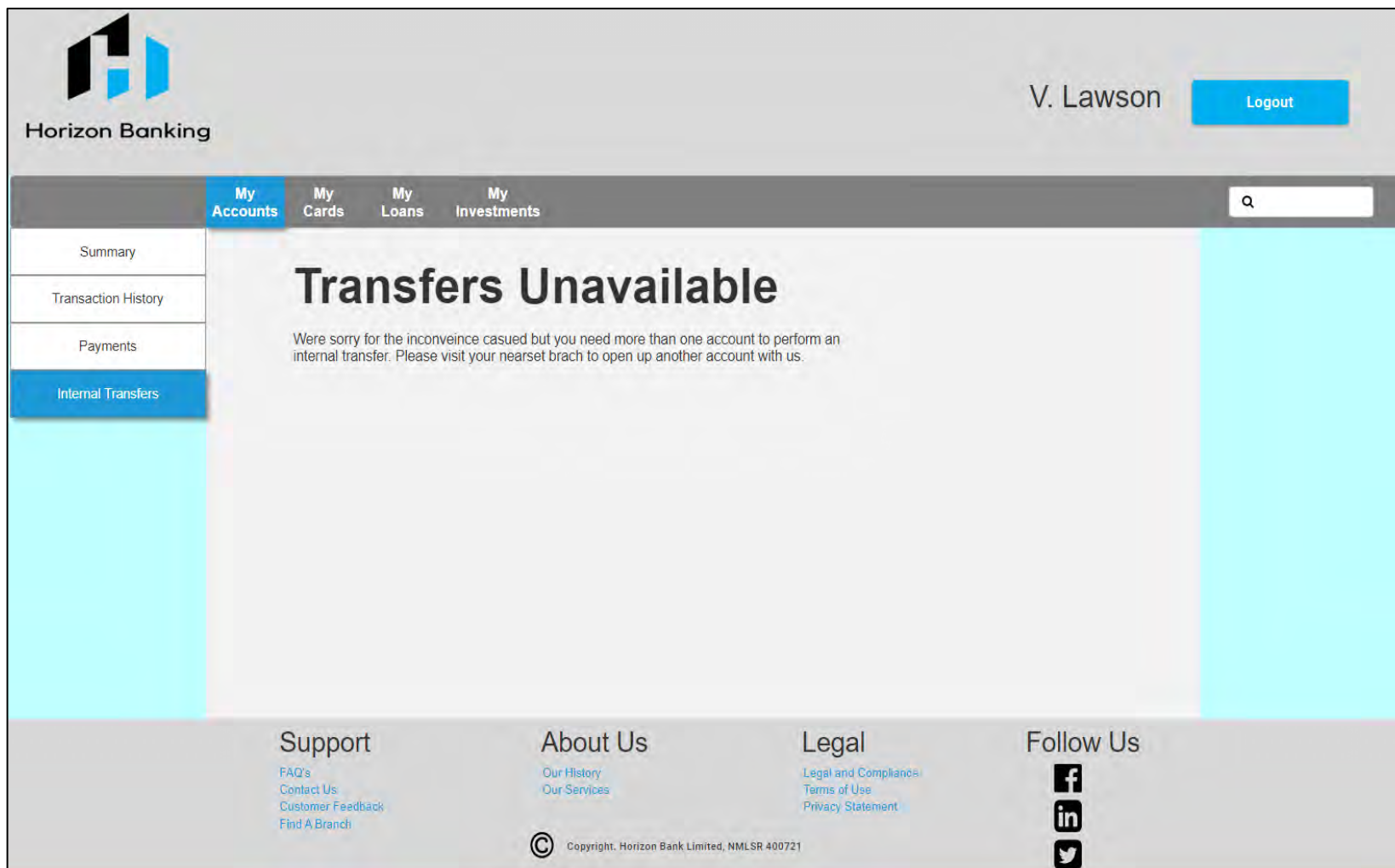



Figure B9: Control and PRE-LOG internal transfers

PRE-LOG



Horizon Banking
INTEGRITY, Convenience, Reliability

PersonalCorporate


[Forgot Username or Password ?](#) [Register](#)


Username:
vallawson@gmail.coi

Password:

Login




AccountsCardsLoansInvestments

Branch/ATM Locator 



Updated Transaction Monitoring System

The system developed by our dedicated Security and Anti-Fraud division monitors client transactions to help detect and prevent fraud. **The system will immediately flag any suspicious or unusual transactions and send an email alert to clients.** Our clients can then use the link provided within the SMS to report and reverse fraudulent transactions.








Figure B10: PRE-LOG homepage top

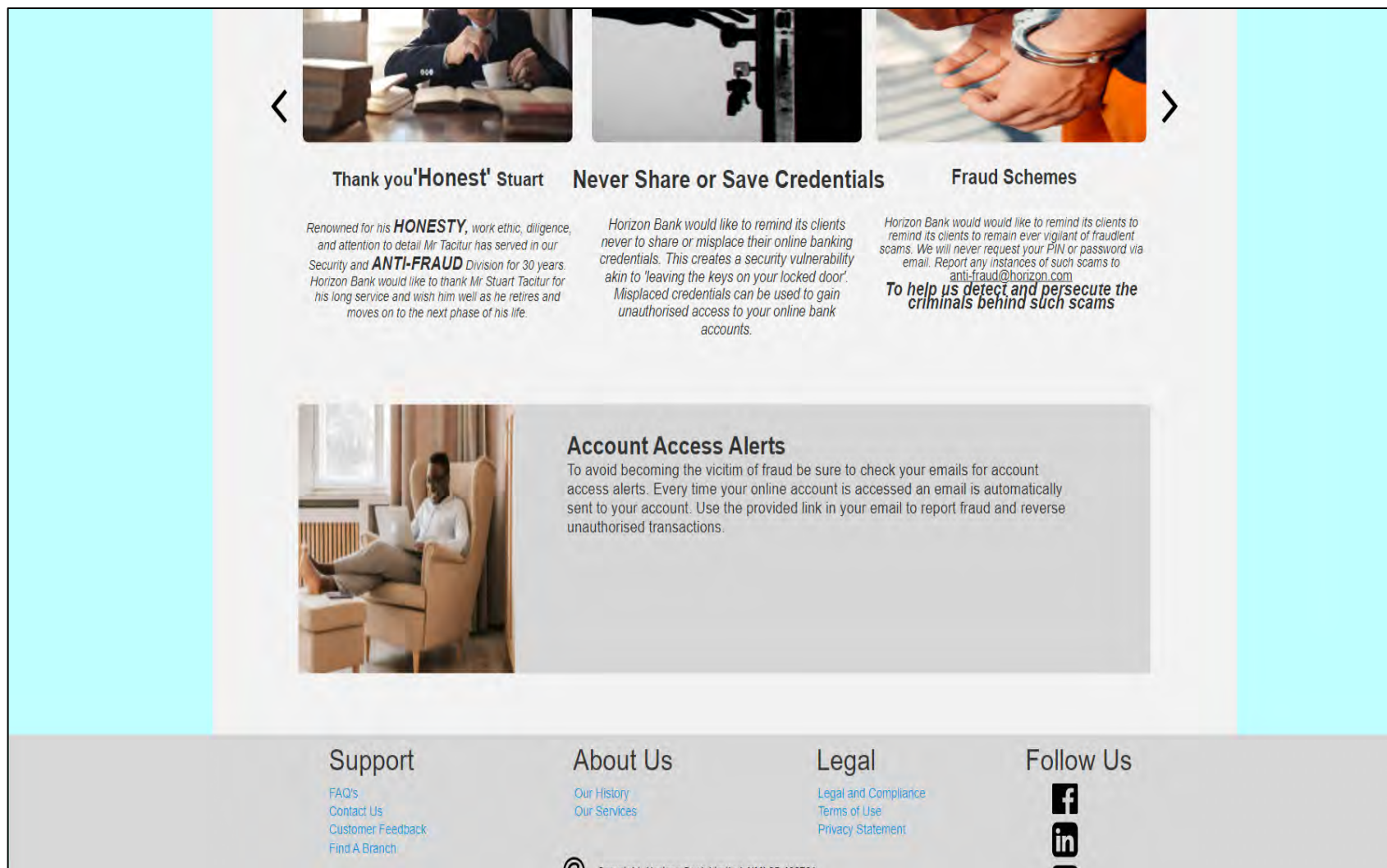




Figure B11: PRE-LOG homepage bottom

POST-LOG



Horizon Banking
INTEGRITY, Convenience, Reliability



V. Lawson


If this isn't you please [Click Here](#)

[Logout](#)

[My Accounts](#)
[My Cards](#)
[My Loans](#)
[My Investments](#)

Branch/ATM Locator

[Summary](#)
[Transaction History](#)
[Payments](#)
[Internal Transfers](#)



Accounts

| <u>First Name(s)</u> | <u>Surname</u> | <u>Account type</u> | <u>Account Number</u> | <u>Balance</u> \$ | <u>Available Balance</u> \$ |
|----------------------|----------------|---------------------|-----------------------|----------------------|--------------------------------|
| Vanessa | Lawson | Checking | 6347300380 | 7722.60 | 7722.60 |

Today's Date 3 July 2022

Support

- [FAQ's](#)
- [Contact Us](#)
- [Customer Feedback](#)
- [Find A Branch](#)




About Us

- [Our History](#)
- [Our Services](#)

Legal


- [Legal and Compliance](#)
- [Terms of Use](#)
- [Privacy Statement](#)

Follow Us


- 
- 
- 

© Copyright: Horizon Bank Limited, NMLSR 400721

Figure B12: POST-LOG summary page



Horizon Banking
INTEGRITY, Convenience, Reliability



V. Lawson
If this isn't you please [Click Here](#)

[Logout](#)

[My Accounts](#)
[My Cards](#)
[My Loans](#)
[My Investments](#)

Branch/ATM Locator

Summary

Transaction History

Payments

Internal Transfers

Vanessa Lawson Today's Date 3 July 2022

Account 6347300380

| Date | Description | Ref | Amount | Checking Account Balance |
|------------|--------------------------|-----------|----------|--------------------------|
| 01-06-2022 | Opening Balance | - | - | 9782.25 |
| 02-06-2022 | Chevron Gas-POS | T1265-622 | (50.27) | 9731.98 |
| 03-06-2022 | Costco Supermarket - POS | T1265-622 | (127.47) | 9604.51 |
| 05-06-2022 | Walgreens Pharmacy - POS | T1265-622 | (300.00) | 9304.51 |
| 10-06-2022 | Costco Supermarket-POS | T3265-622 | (85.67) | 9218.84 |
| 12-06-2022 | Grandson Gift | T3369-622 | (100) | 9118.84 |
| 16-06-2022 | Costco Supermarket - POS | T3532-622 | (127.47) | 8991.37 |

[Previous](#)
[1](#)
[2](#)
[3](#)
[Next](#)

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)




About Us

[Our History](#)
[Our Services](#)

Legal


[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)

Follow Us






© Copyright. Horizon Bank Limited, NMLSR 400721

Figure B13: POST-LOG transaction history (page 1)



Horizon Banking
INTEGRITY, Convenience, Reliability



V. Lawson
If this isn't you please [Click Here](#)

Logout

My Accounts

My Cards

My Loans

My Investments

Branch/ATM Locator

Summary

Transaction History

Payments

Internal Transfers

Vanessa Lawson Today's Date: 3 July 2022

Account 6347300380 Account Type : **Checking Account**

| Date | Description | Ref | Amount | Balance |
|------------|-------------------------|-----------|----------|---------|
| 17-06-2022 | NetflixUSA | T3282-622 | (19.99) | 8971.38 |
| 20-06-2022 | Cappellini's Restaruant | T4368-622 | (60.00) | 8911.38 |
| 21-06-2022 | Costco-Supermarket-POS | T4578-622 | (64.25) | 8847.13 |
| 22-06-2022 | ChevronGas | T5687-622 | (89.99) | 8757.14 |
| 23-06-2022 | Walgreens Pharmacies | T5702-622 | (300.00) | 8457.14 |
| 24-06-2022 | Axis Health Insurance | T5421-622 | (340.00) | 8117.14 |
| 25-06-2022 | Monthly Medical Checkup | T5265-452 | (50) | 8067.14 |

[Previous](#)
[1](#)
[2](#)
[3](#)
[Next](#)

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)




About Us

[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)

Follow Us




 Copyright: Horizon Bank Limited, NMLSR 400721

Figure B14: POST-LOG transaction history (page 2)



Horizon Banking
INTEGRITY, Convenience, Reliability



V. Lawson
If this isn't you please [Click Here](#)

[Logout](#)

[My Accounts](#)
[My Cards](#)
[My Loans](#)
[My Investments](#)

Branch/ATM Locator

[Summary](#)
[Transaction History](#)
[Payments](#)
[Internal Transfers](#)

Vanessa Lawson

Today's Date 3 July 2022

Account 6347300380 **Account Type :** **Checking Account**

| Date | Description | Ref | Amount | Balance |
|------------|----------------------|-----------|----------|---------|
| 25-06-2022 | Electric Bill | T5639-622 | (284.54) | 7782.60 |
| 26-06-2022 | City-Rates | T4654-622 | (60.00) | 7722.60 |
| 30-06-2022 | Closing Balance June | - | - | 7722.60 |
| 01-07-2022 | Opening Balance July | - | - | 7722.60 |

[Previous](#)
[1](#)
[2](#)
[3](#)
[Next](#)

Support

- [FAQ's](#)
- [Contact Us](#)
- [Customer Feedback](#)
- [Find A Branch](#)




About Us

- [Our History](#)
- [Our Services](#)

Legal


- [Legal and Compliance](#)
- [Terms of Use](#)
- [Privacy Statement](#)

Follow Us






© Copyright. Horizon Bank Limited, NMLSR 400721

Figure B15: POST-LOG transaction history (page 3)



Horizon Banking
 INTEGRITY, Convenience, Reliability



V. Lawson
 If this isn't you please [Click Here](#)

Logout

My Accounts

My Cards

My Loans

My Investments

Branch/ATM Locator 0

Summary

Transaction History

Payments

Internal Transfers

Add Recipient

| Recipient Name | Bank | Account Num | My Ref | Last Paid |
|-----------------------|-----------------|--------------|-------------------------|------------------|
| Samuel Lawson | Bank Of America | 263956958524 | Grandson Gift | 12 June 2022 |
| St Luke's Hospital | Bank of America | 256214545254 | Monthly Medical Checkup | 25 June 2022 |
| Craybar Mechanics | Capital One | 123565849875 | CarService | 13 February 2022 |
| Axis Health Insurance | Capital One | 123669854562 | Health Insurance | 24 June 2022 |
| Blueline Energy INC | Wells Fargo | 265898681524 | ElectricBill | 25 June 2022 |
| Bob Parr | Bank of America | 123123213 | Bobby Parr | |

Support

About Us

Legal

Follow Us

FAQ's
 Contact Us
 Customer Feedback
 Find A Branch


Our History
 Our Services

Legal and Compliance
 Terms of Use
 Privacy Statement


f
 in
 t

© Copyright. Horizon Bank Limited, NMLSR 400721

Figure B16: POST-LOG payments page



Horizon Banking
INTEGRITY, Convenience, Reliability



V. Lawson
If this isn't you please [Click Here](#)

Logout

My Accounts

My Cards

My Loans

My Investments

Branch/ATM Locator 0

Summary

Transaction History

Payments

Internal Transfers

Default Payment Account

Account

Recipient Details

Recipient Name

Bank ?

Account Number ?

My Reference ?

Proof of Payment

Email Address ?

CANCEL ?

ADD Recipient

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)




About Us

[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)

Follow Us




 Copyright. Horizon Bank Limited, NMLS# 400721

Figure B17: POST-LOG add recipients form



Horizon Banking
INTEGRITY, Convenience, Reliability



V. Lawson
If this isn't you please [Click Here](#)

Logout

My AccountsMy CardsMy LoansMy Investments

Branch/ATM Locator

SummaryTransaction HistoryPaymentsInternal Transfers

Make Payment to Bob Parr

Select Account

Checking Account- 6347300380

Amount

4000

Pay And Clear Now

☒ Yes
☐ No

Cancel

?

Make Payment

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)

About Us

[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)

Follow Us





© Copyright: Horizon Bank Limited, NMLSR 400721

Figure B18: POST-LOG pay recipient form

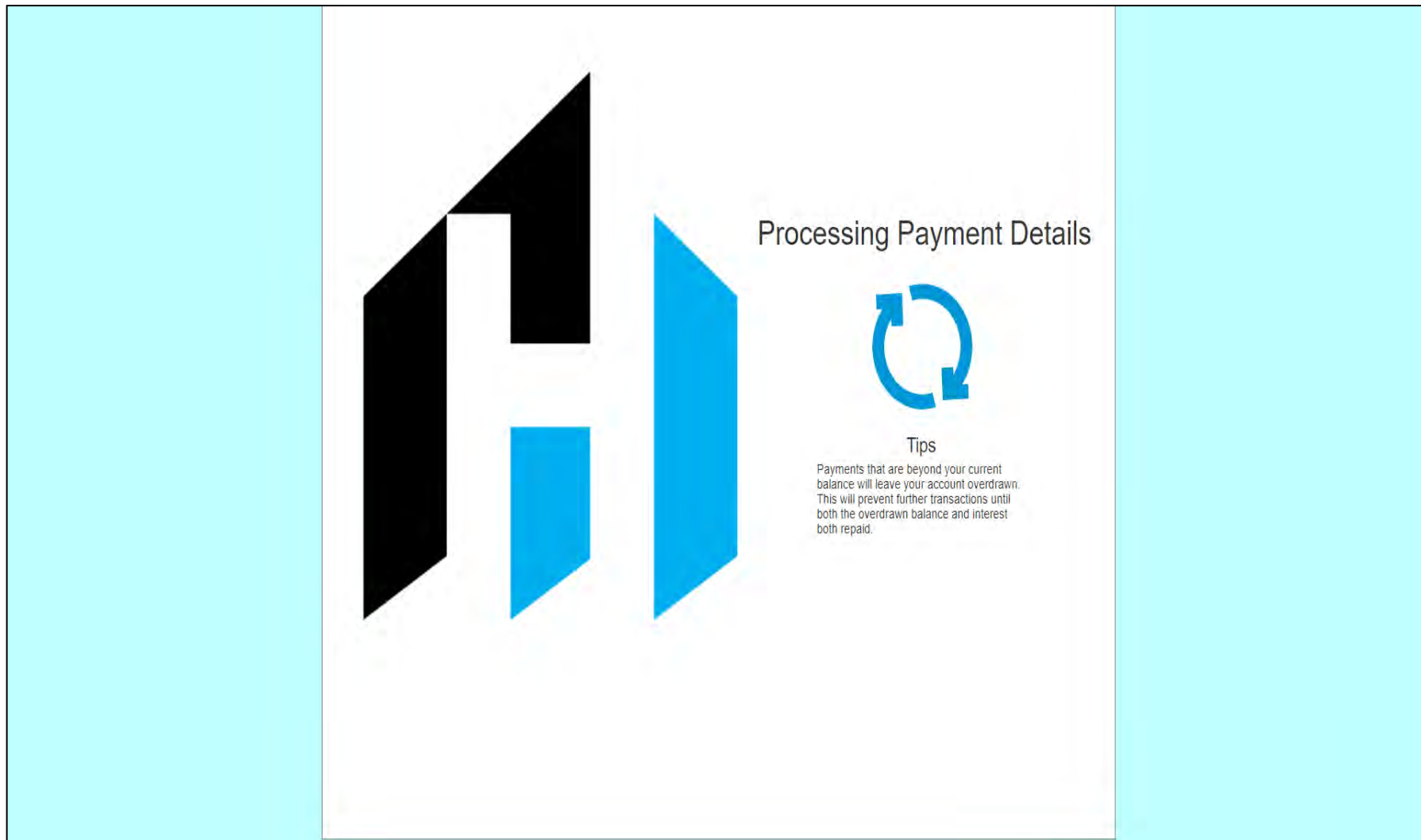




Figure B19: POST-LOG payment processing



Horizon Banking
INTEGRITY, Convenience, Reliability



V. Lawson
If this isn't you please [Click Here](#)

[Logout](#)

[My Accounts](#)
[My Cards](#)
[My Loans](#)
[My Investments](#)

Branch/ATM Locator

[Summary](#)
[Transaction History](#)
[Payments](#)
[Internal Transfers](#)

Confirm payment to Bob Parr?

Be aware Vanessa, completing this transaction will reduce account balance of Checking Account- 6347300380 by 400000 cents. Even with the resultant reduction in funds in your account do you still wish to proceed with the transaction.

Device and Payment Request details recorderd

[CANCEL](#)
[?](#)

[CONFIRM](#)

Support

[FAQ's](#)
[Contact Us](#)
[Customer Feedback](#)
[Find A Branch](#)




About Us

[Our History](#)
[Our Services](#)

Legal

[Legal and Compliance](#)
[Terms of Use](#)
[Privacy Statement](#)

Follow Us







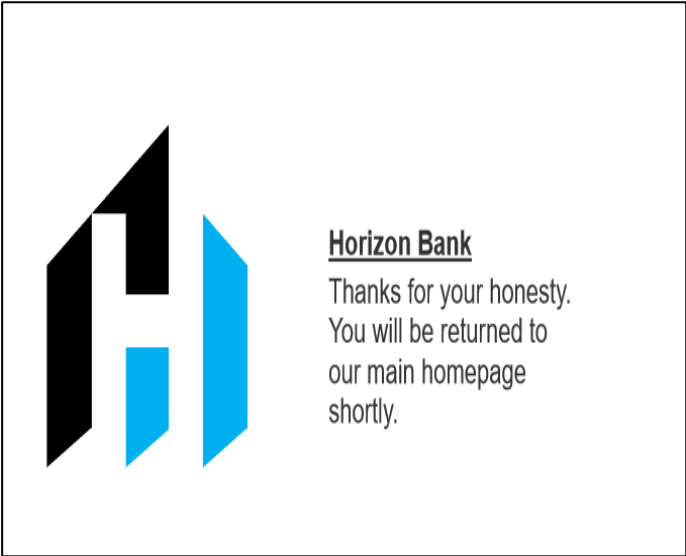
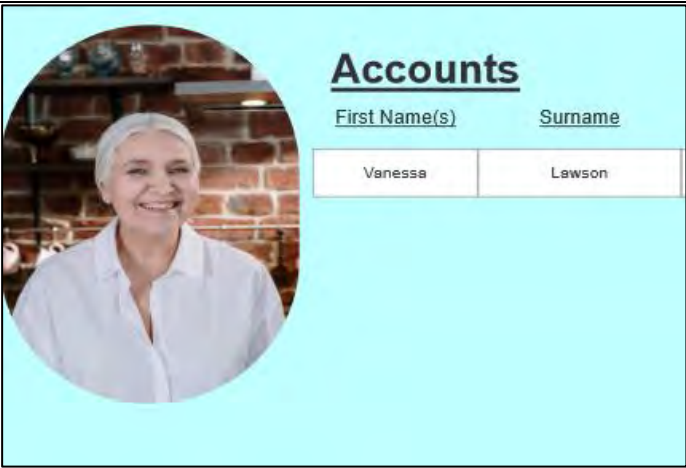
© Copyright Horizon Bank Limited, NMLSR 400721

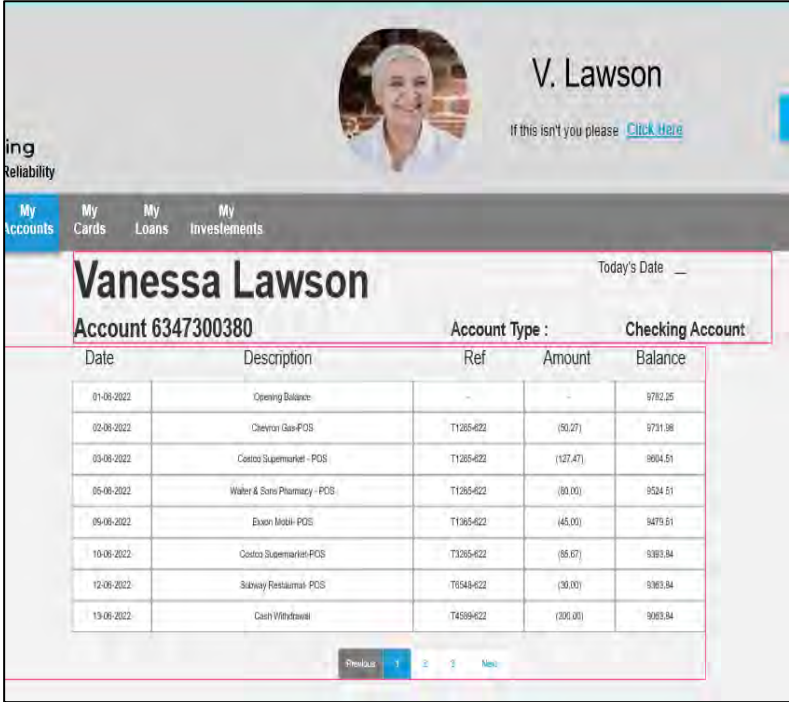
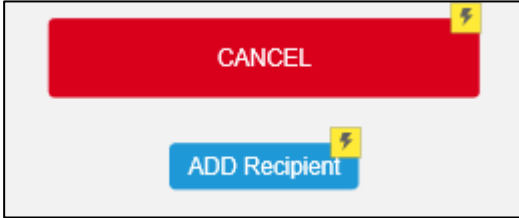
Figure B20: POST-LOG payments confirmation page

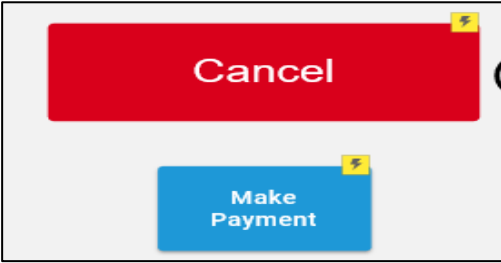
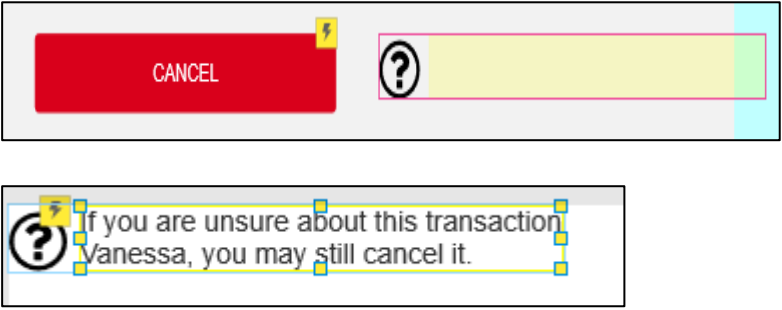
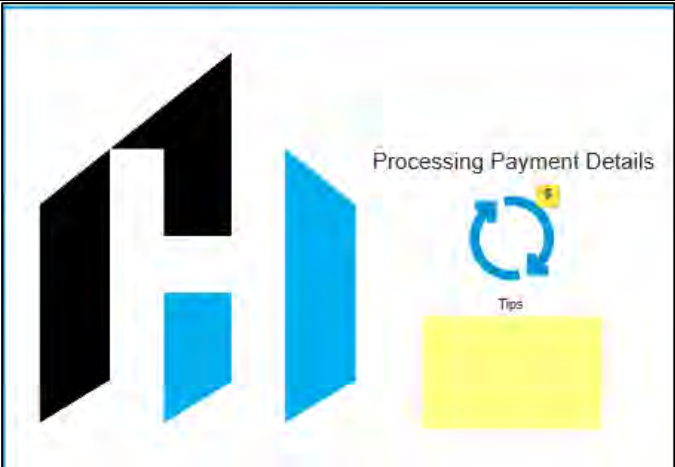
Nudge Mechanisms Used

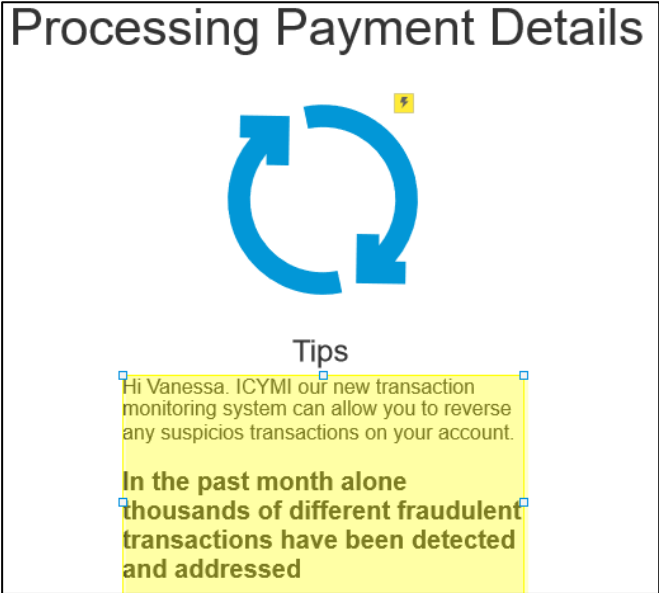
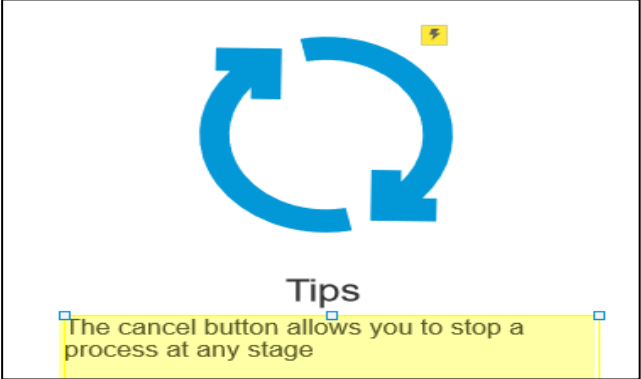
Table B1: POST-LOG nudges

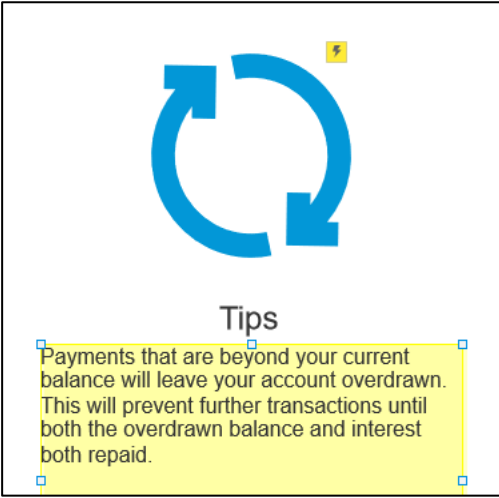
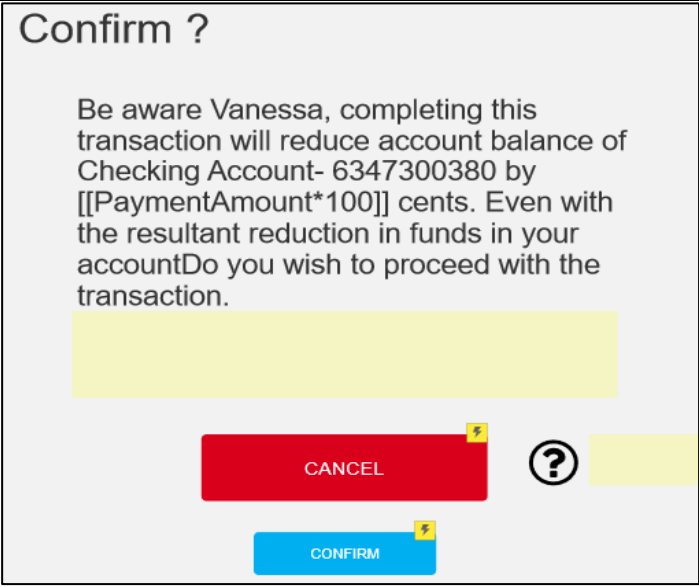
| Nudge (screenshot) | Nudge mechanism | Website version | COM-B factor |
|--|---|-----------------|-------------------------------------|
|  | <p>“Remind of socially desirable concepts”, salience, and priming:</p> <ul style="list-style-type: none"> The slogan below the company logo acts as a constant reminder to be honest. Social norm(s)/value(s) of integrity are brought up. Since it is ever present across the interface, it acts as a prime, even if only read once. Integrity is put in CAPS to stand out on this interface. | POST-LOG | Capability, opportunity, motivation |
|  | <p>Instigate empathy (‘Instigate empathy with characters’ and ‘Invoking feelings of reciprocity’), reminder</p> <ul style="list-style-type: none"> The account holder's picture in the header is a constant reminder to unauthorised visitors. “Click Here” is constant to give unauthorised users the option to leave the website at any stage. | POST-LOG | Capability, opportunity, motivation |

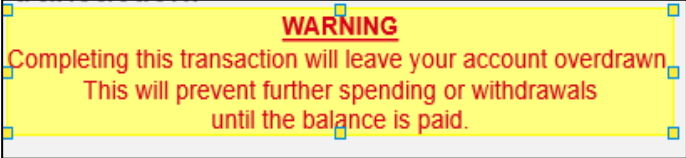
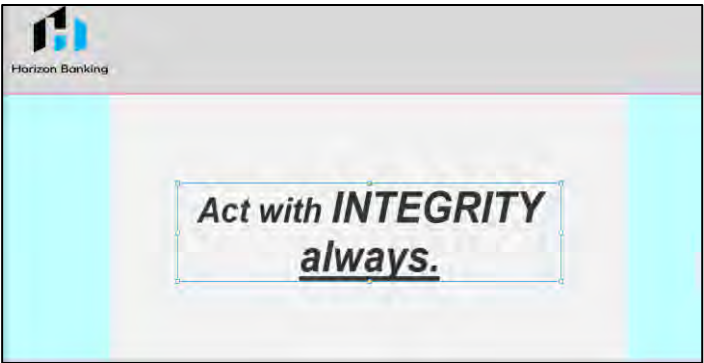
| Nudge (screenshot) | Nudge mechanism | Website version | COM-B factor |
|--|--|-----------------|-------------------------------------|
|  | <p>Positive reinforcement</p> <ul style="list-style-type: none"> Users' honesty is acknowledged after they use "Click Here" in the header. | POST-LOG | Capability, opportunity |
|  | <p>Instigate empathy ('Instigate empathy with characters' and 'Invoking feelings of reciprocity')</p> <ul style="list-style-type: none"> Picture of the account holder (full-sized now) is meant to give unauthorised users a better picture of the victim (account holder) if they do end up committing fraud. Put a face to the name they constantly see. | POST-LOG | Capability, opportunity, motivation |

| Nudge (screenshot) | Nudge mechanism | Website version | COM-B factor |
|---|---|-----------------|-------------------------------------|
|  <p>The screenshot shows a banking website interface. At the top, there's a user profile for 'V. Lawson' with a circular photo and a link 'Click Here' with the text 'If this isn't you please'. Below this is a navigation bar with 'My accounts', 'My Cards', 'My Loans', and 'My Investments'. The main section displays 'Vanessa Lawson' and 'Account 6347300380' with 'Account Type: Checking Account'. A table shows transaction history with columns: Date, Description, Ref, Amount, and Balance. The table lists transactions from 01-06-2022 to 19-06-2022, including 'Opening Balance', 'Chevron Gas-POS', 'Costco Supermarket - POS', 'Walter & Sons Pharmacy - POS', 'Buxon Mobil-POS', 'Costco Supermarket-POS', 'Subway Restaurant-POS', and 'Cash Withdrawal'.</p> | <p>Instigate empathy ('Instigate empathy with characters' and 'Invoking feelings of reciprocity')</p> <ul style="list-style-type: none"> Transaction history gives an insight into the account holder's life and spending patterns. While present on all three versions of the website, the empathy aspect is more apparent on the POST-LOG version due to the presence of the account holder's picture. Account transactions in the POST-LOG version have also been altered to generate more sympathy with "Vanessa" and her sweet old lady image. | POST-LOG | Capability, opportunity, motivation |
|  <p>The screenshot shows a form with two buttons. At the top is a red button labeled 'CANCEL'. Below it is a blue button labeled 'ADD Recipient'. Both buttons have a small yellow lightning bolt icon in the top right corner.</p> | <p>"Salience (ordering)" and "positioning".</p> <ul style="list-style-type: none"> The cancel button is placed in a location that breaks the normal flow (reading form, then option to confirm/submit is the normal flow). Placing it before adding the recipient makes it more salient and nudges the user to cancel. | POST-LOG | Capability |

| Nudge (screenshot) | Nudge mechanism | Website version | COM-B factor |
|--|--|-----------------|-------------------------------------|
|  | <p>Salience (deceptive visualisations) and positioning</p> <ul style="list-style-type: none"> The size of the cancel button is significantly larger than the other button. It nudges the user towards cancelling the transaction or process. | POST-LOG | Capability, motivation |
|  | <p>Reminder and “situated”</p> <ul style="list-style-type: none"> The user, authorised or not, always has the option to cancel a transaction. It displays when the page opens and when the question mark icon is hovered over. | POST-LOG | Capability |
|  | <p>Speed bump</p> <ul style="list-style-type: none"> The user is forced to slow down and think a little while completing a payment. Cycles through three “tip messages” as the user waits for the payment details to be processed. <p>Friction</p> <ul style="list-style-type: none"> Tips messages place reminders just before the user decides on the alternate path they may take; in other words, avoiding committing online banking fraud. | POST-LOG | Capability, opportunity, motivation |

| Nudge (screenshot) | Nudge mechanism | Website version | COM-B factor |
|--|---|-----------------|------------------------|
|  | <p>“Reduce the distance” and “optimism and overconfidence”</p> <ul style="list-style-type: none"> Tip 1: The text in bold is designed to make an authorised user less sure of their chances of committing fraud undetected. <p>Reminder (salience of consequences) and “reduce the distance”</p> <ul style="list-style-type: none"> One of many repeated reminders about the monitoring of transactions. It helps reduce the distance by making it more apparent that unauthorised users like the third party were detected and most likely prosecuted in the past. Hints that past unauthorised users have been caught and punished before (salience of consequences). | POST-LOG | Capability, motivation |
|  | <p>Reminder</p> <ul style="list-style-type: none"> Tip 2: Gives all users a reminder that they can opt out and stop any process/transaction. <p>Friction</p> <ul style="list-style-type: none"> This specific tip explicitly reminds them that they could turn back as the cancel button has been available as an option on all the pages they have encountered. The cancel button is present on the page. | POST-LOG | Capability, motivation |

| Nudge (screenshot) | Nudge mechanism | Website version | COM-B factor |
|--|---|-----------------|-------------------------------------|
|  | <p>“Warning”, “reminder”, and “connect decision benefit/cost.”</p> <ul style="list-style-type: none"> Tip 3: It makes it apparent that it is possible to deplete and overdraw the account, leaving the account holder with an overdraft. | POST- LOG | Capability, motivation |
|  | <p>“Change scale”</p> <ul style="list-style-type: none"> The amount to be paid is expressed in cents to overemphasise (exaggerate) its impact. <p>“Framing” and “loss aversion”</p> <ul style="list-style-type: none"> Reducing the account’s balance paints the payment transaction in a very negative light. Payment is phrased in such a way that the account holder is left worse off. An alternative would have been to phrase the transaction regarding what the recipient gains. <p>Connect decision to benefit/cost</p> <ul style="list-style-type: none"> Payment’s impact is shown via the balance reduction aspect of the message. | POST-LOG | Capability, opportunity, motivation |

| Nudge (screenshot) | Nudge mechanism | Website version | COM-B factor |
|--|---|-----------------|-------------------------------------|
| | <p>Prompted choice</p> <ul style="list-style-type: none"> Users can confirm or cancel the transaction. <p>“Changing ease and convenience” and “enhancing or influencing active choosing”</p> <ul style="list-style-type: none"> The extra step of confirming payment is only available on the POST-LOG version of the website. The prompt forces users to confirm their payment, unlike the control, which skips straight ahead to the recipient’s page. Prompt combined with the other mentioned nudges. | | |
|  | <p>“Warning”, “reminder”, and “Connect decision benefit/cost”</p> <ul style="list-style-type: none"> It should only appear when the user’s transaction threatens to leave the account overdrawn. | POST-LOG | Capability, motivation |
|  | <p>“Priming” (subliminal), and “remind of socially desirable values”</p> <ul style="list-style-type: none"> After logging in, the message appears briefly before opening the first page (summary). | POST-LOG | Capability, opportunity, motivation |

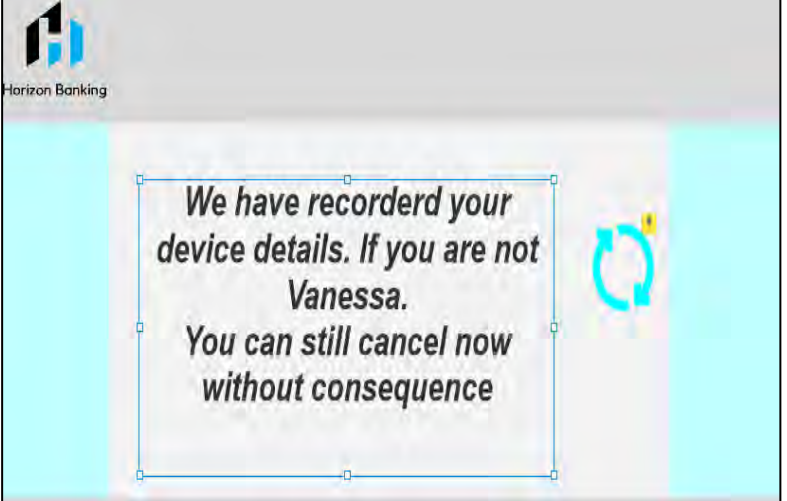
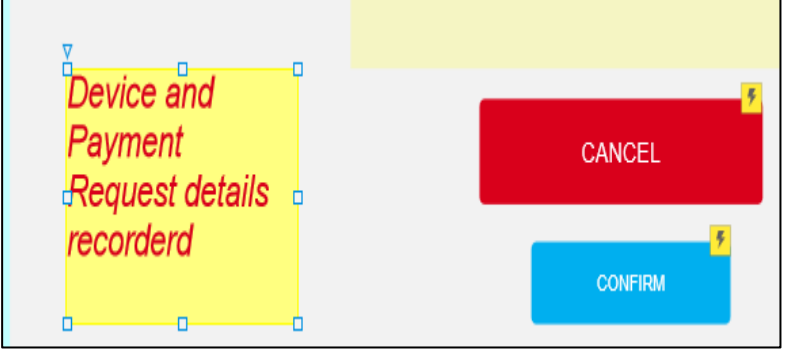


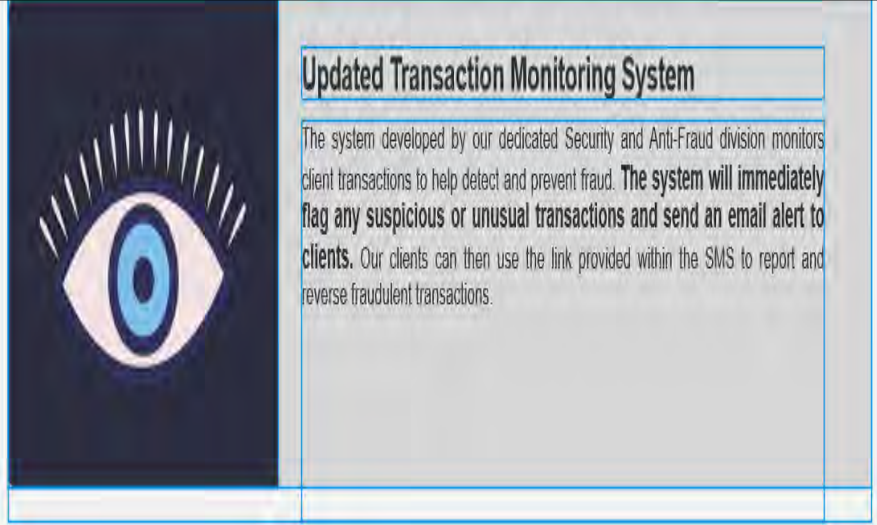




| Nudge (screenshot) | Nudge mechanism | Website version | COM-B factor |
|--|---|-----------------|------------------------|
|  | <p>“Priming”, “warning”, and “reduce the distance.”</p> <ul style="list-style-type: none"> • The message appears briefly (roughly 1-3 seconds) to try to dissuade potential fraudulent actions on the website (prime). The message pops up when first trying to access the local navigation of the POST-LOG interface. • The message itself warns that the account's transactions are being observed. This also helps reduce distance as the message directly addresses the (unauthorised) user. • Chances of being caught/detected seem much higher as the message almost directly addresses the unauthorised user. | POST-LOG | Capability, Motivation |
|  | <p>“Reduce the distance”, “warning”, and “situated”</p> <ul style="list-style-type: none"> • I want the unauthorised user to think if they have recorded my details, they can probably track me down too. • The message is displayed in the style (yellow background red text) of other warnings. The style of the warning is meant to make it stand out. • A message appears briefly, then disappears again. It can reappear when the confirm button is hovered over. | POST-LOG | Capability, Motivation |


Table B2: PRE-LOG nudges

| Nudge (screenshot) | Nudge mechanism | Website version | COM-B factor |
|---|---|-----------------|-------------------------------|
| <p>Updated transaction monitoring system</p> <p>Horizon Bank would like to remind its clients about our updated transaction monitoring system. The new system developed by our dedicated Fraud and Security team allows all transactions to be monitored. Suspicious or unusual transactions are flagged.</p> <p>Any transaction flagged as suspicious will send have an SMS alert sent to the respective clients cellphone. Clients can open the included link to begin the process of reporting and reversing fraudulent transactions.</p>  | <p>“Spotlight effect” and “salience”</p> <ul style="list-style-type: none"> • This page only appears after logging in to the POST-LOG version of the website. • Part of the text was made bold and larger to increase its salience. • The message on this page is meant to make users believe that transactions are monitored very carefully (spotlight effect); thus reducing the chances of getting away with unauthorised transactions (fraud). | <p>PRE- LOG</p> | <p>Capability, motivation</p> |

| | | | |
|---|---|--|---|
|  <p data-bbox="353 336 931 400">DON'T Impersonate</p> | <p data-bbox="1200 196 1440 225">Priming (subliminal)</p> <ul data-bbox="1200 248 1675 456" style="list-style-type: none"> • Warning page appears briefly as you open the PRE-LOG homepage and right after logging in. • Meant to stick in the back of one's thoughts as they transact on the website. | <p data-bbox="1697 196 1823 225">PRE-LOG</p> | <p data-bbox="1877 196 2002 225">Motivation</p> |
|  <p data-bbox="510 667 907 711">Updated Transaction Monitoring System</p> <p data-bbox="510 738 1037 922">The system developed by our dedicated Security and Anti-Fraud division monitors client transactions to help detect and prevent fraud. The system will immediately flag any suspicious or unusual transactions and send an email alert to clients. Our clients can then use the link provided within the SMS to report and reverse fraudulent transactions.</p> | <p data-bbox="1200 614 1675 679">Spotlight effect, order effects (positioning), salience, and priming</p> <ul data-bbox="1200 703 1675 1222" style="list-style-type: none"> • This is one of the first things a user should spot when opening the page. • It has been deliberately moved and placed above the normal image carousel shown on the (control) version. • Transaction monitoring is meant to spook visitors to the site by making them believe that transactions are being monitored carefully; thus raising the chances of fraud being detected. • The text regarding the monitoring system is in bold to make it more apparent to visitors. | <p data-bbox="1697 614 1823 643">PRE-LOG</p> | <p data-bbox="1877 614 2002 679">Capability, motivation</p> |

| | | | | |
|---|--|---|---------|-------------------------------------|
|  <p>Thank you 'Honest' Stuart</p> <p>Renowned for his HONESTY, work ethic, diligence, and attention to detail Mr Tacit has served in our Security and ANTI-FRAUD Division for 30 years. Horizon Bank would like to thank Mr Stuart Tacit for his long service and wish him well as he retires and moves on to the next phase of his life.</p> | | <p>“Remind of socially desirable values” and “salience”</p> <ul style="list-style-type: none"> • The words “honest” and “anti-fraud” are bold and resized to be bigger than the surrounding text. • “Honest” and “anti-fraud” are meant to evoke general social norms/values about not stealing. | PRE-LOG | Capability, motivation, opportunity |
|  <p>Never Share or Save Credentials</p> <p>Horizon Bank would like to remind its clients never to share or misplace their online banking credentials. This creates a security vulnerability akin to 'leaving the keys on your locked door'. Misplaced credentials can be used to gain unauthorised access to your online bank accounts.</p> | | <p>“Reminder”</p> <ul style="list-style-type: none"> • Unique in that it is more aimed towards the authorised Horizon Bank client. • It was meant to make it seem like Horizon Bank is already aware of such instances of fraud, hopefully causing some cause for concern for unauthorised third parties. | PRE-LOG | Motivation |

| | | | |
|--|--|---------|------------------------|
|  <p>S Fraud Schemes</p> <p>Horizon Bank would like to remind its clients to remind its clients to remain ever vigilant of fraudulent scams. We will never request your PIN or password via email. Report any instances of such scams to anti-fraud@horizon.com</p> <p>To help us detect and persecute the criminals behind such scams</p> | <p>Warning, salience, priming, and “connect decision to benefit/cost”</p> <ul style="list-style-type: none"> • The goal is to get a third party to make the association between fraud and prosecution. • Warns unauthorised users of the risks of transacting. | PRE-LOG | Capability, motivation |
|  <p>Account Access Alerts</p> <p>To avoid becoming the victim of fraud be sure to check your emails for account access alerts. Every time your online account is accessed an email is automatically sent to your account. Use the provided link in your email to report fraud and reverse unauthorised transactions.</p> | <p>“Salience” and “spotlight effect”</p> <ul style="list-style-type: none"> • Alerts give a reminder that accessing this account will be recorded by the system. The goal is to make the unauthorised user feel unsure about how they could get away with it. • The alerts message and “report fraud” are bolded to ensure they stand out. | PRE-LOG | Capability, motivation |

| | | | | |
|---|--|---|---------|-------------------------|
|  | | <p>“Remind of socially desirable concepts”</p> <ul style="list-style-type: none"> • Slogan below the company logo acts as a constant reminder to be honest. Social norm(s)/value(s) of integrity are brought up. | PRE-LOG | Motivation, opportunity |
|---|--|---|---------|-------------------------|

APPENDIX C: INTERVIEW QUESTIONS

- ☐ Open meeting
- ☐ Activate live transcription
- ☐ Rename participant
- ☐ Activate meeting recording (record to the cloud)

☐ **Greeting**

Thank you for taking the time to participate in this research project. How are you doing today?

☐ **Preface**

This project is being carried out as part of the requirements for completing a master's degree at Rhodes University in South Africa. [Start off with basic demographic questions, then explain the intro.]

☐ **Basic demographic questions**

- What is your gender?
- What is your age?
- What is your educational background (highest level achieved)?

☐ **Subsequent interview quick explanation**

Interact with three versions of a fictitious online banking website. The Control, the PRE-LOG, and the POST-LOG version at various points during the interview. **Control** will be a **tutorial** on the website and what can be interacted with.

PRE-LOG: Nudges situated on the homepage before hitting the logon button.

POST-LOG: Nudges situated after hitting logging in and gaining access.

Questions asked are going to focus on the **rationalisations and behaviour** of a hypothetical third party in the scenario(s). Once done with all three sites and their questions, there will be a short debrief.

Main scenario (third party)

Jack/Jill Taylor was recently involved in a small car accident. They've gone to visit their local Internet café to browse the web in search of an affordable local mechanic to repair their car. Besides Jack/Jill Taylor, there isn't another customer in the café. While walking past, Jack/Jill notices one of the machines is on and has an online banking website open. The credentials are on a sticky note under the keyboard.

- ☐ Share the control version screen.
 - ☐ Explain inactive parts.
 - ☐ Credentials to log in are in the Chat or "sticky note" (need to be typed in).
 - ☐ Give you **remote control** of the control version of the website.
 - ☐ Activate macro recorder.
 - ☐ Short tutorial on adding recipients and making payments.
 - ☐ **Revoke the remote control** on the page.
 - ☐ Deactivate macro recorder (save recording).
 - ☐ Stop sharing.
 - ☐ Questions.
-
- Given what you have seen on this version of the interface, what do you think Jack/Jill would do if they encountered it along with the credentials?
 - What would Jack/Jill's thought process (or rationalisation) be when making that decision?

THAT'S IT FOR CONTROL.

PRE-LOG scenario modification

While walking past, Jack/Jill notices that one of the machines is on and has an online banking homepage open. Jack/Jill also notices that the online banking credentials seem to have been saved on the machine.

- ☐ Share the PRE-LOG version.
 - ☐ **Activate macro recorder (save previous recording).**
 - ☐ Give **remote control**.
 - ☐ Play the role of Jack/Jill.
 - ☐ **Deactivate** macro recorder (save recording).
 - ☐ **Revoke remote control**.
 - ☐ Questions.
-
- Jack/Jill did _____!
 - Would they also commit an unauthorised transaction?
 - What was Jack/Jill's thought process or rationalisations for deciding to do that (hit login) (or transact)?
 - Going back to the homepage of the interface, what aspect(s) or feature(s) would have stood out the most to Jack/Jill?
 - Anything else on the page that may have stood out to Jack/Jill or affected their decision/behaviour?
-

THAT'S IT FOR THE PRE-LOG.

STOP SHARING PRE-LOG.

POST-LOG scenario modification

While walking past, Jack/Jill notices one of the machines is on and has an online banking website open. Jack/Jill Taylor also notices the previous user forgot to log out out of their account!

- ☐ Share the POST-LOG version.
- ☐ Activate **macro recorder**.
- ☐ Give **remote control**.
- ☐ Play the role of Jack/Jill.
- ☐ **Revoke remote control**.
- ☐ **Deactivate macro recorder (save recording)**.
- ☐ Questions.

- Jack/Jill did _____!
- What was Jack/Jill's thought process or rationalisations for deciding to do that click (or transact)?
- Looking back to the pages you encountered on the pages you encountered in this POST-LOG version, would any feature(s) or aspects(s) have stood out to Jack/Jill?

THAT'S IT FOR THE POST-LOG VERSION.

STOP SHARING.

- Looking back between the PRE-LOG and POST-LOG versions, which version could have had the more significant effect on **Jack/Jill's** behaviours and rationalisations? Why?
- If both versions (halves) were combined, how would this impact the behaviour and rationalisations of **Jack/Jill?** (If it makes any difference at all?)
- Which aspect on all three versions (specifically fraud, yes) had the most effect on **Jack/Jill's** behaviour

DEBRIEF

☐ In summary:

- On Control, **Jack/Jill** would do _____ because of _____
- On PRE-LOG, **Jack/Jill** would do _____ because of _____
- On POST-LOG, **Jack/Jill** would do _____ because of _____

☐ Confidentiality update:

- The data collected during this meeting will be saved on a password-protected cloud storage account. Before I get to analysing the data, I will review it to make it anonymous, and make sure that nothing ties back to you.

☐ The data collected from all the interviews will be used to complete my thesis.

☐ The remuneration (bonus payment) should be done within the next day or two.

☐ Thanks again for taking the time to participate and help me with my research.

☐ Have a great day!

END

APPENDIX D: MAPS

CONTROL



Figure D1: Thought process and rationalisations (Control) project map (Phase 2 of Braun and Clarke, 2006)

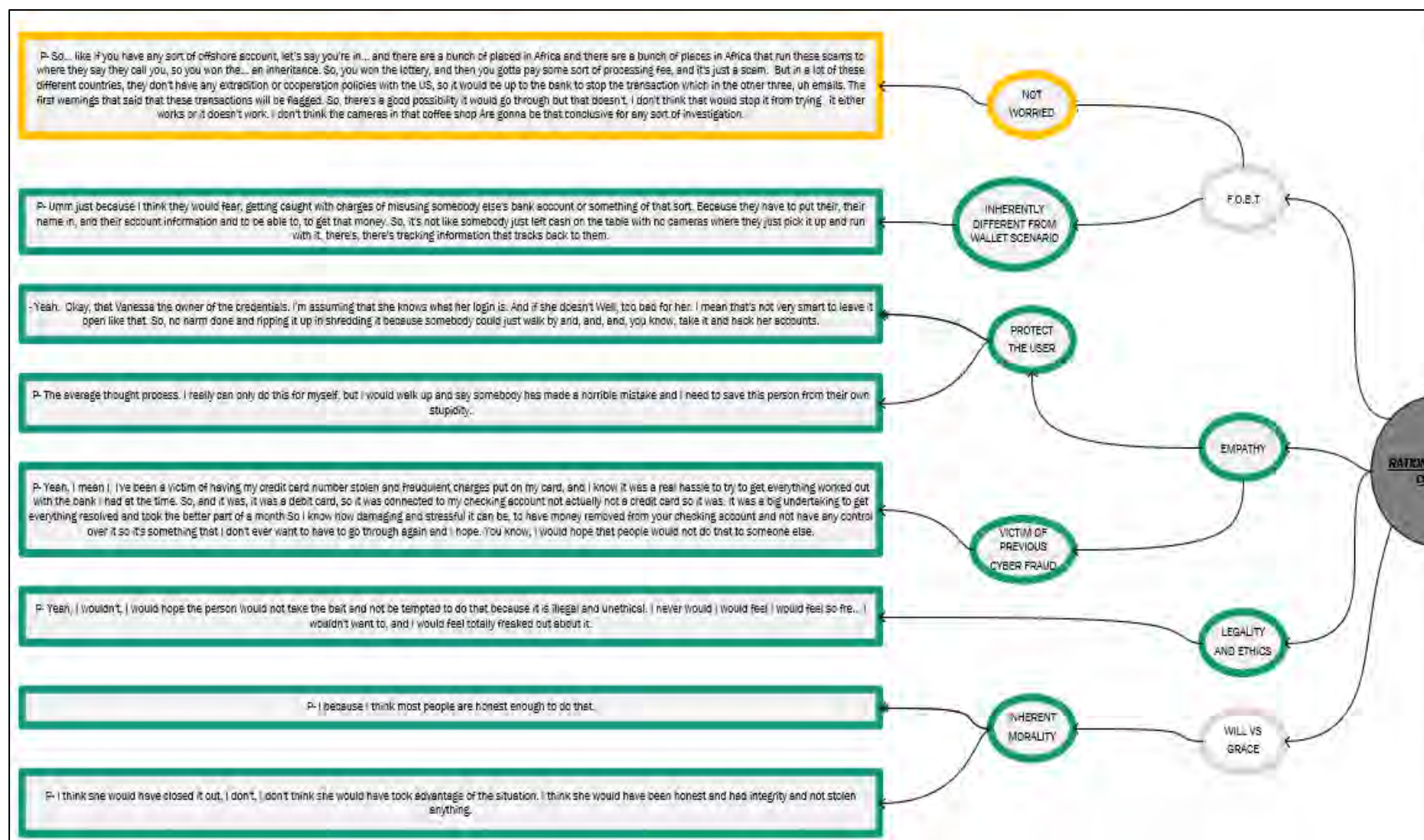


Figure D2: Initial thematic map (Control) thought process and rationalisations: left side (Phase 3)

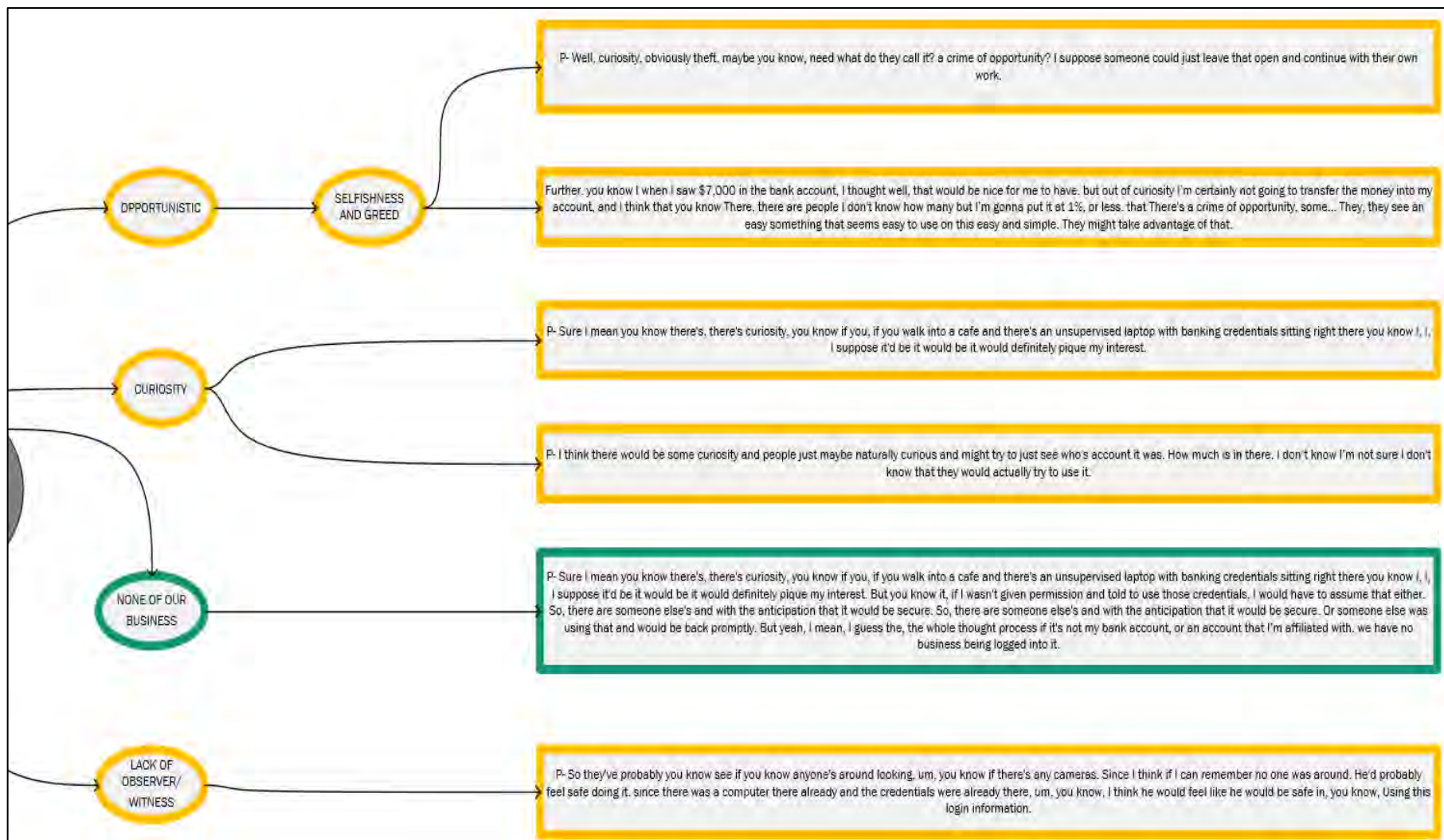


Figure D3: Initial thematic map (Control) thought process and rationalisations: right side (Phase 3)

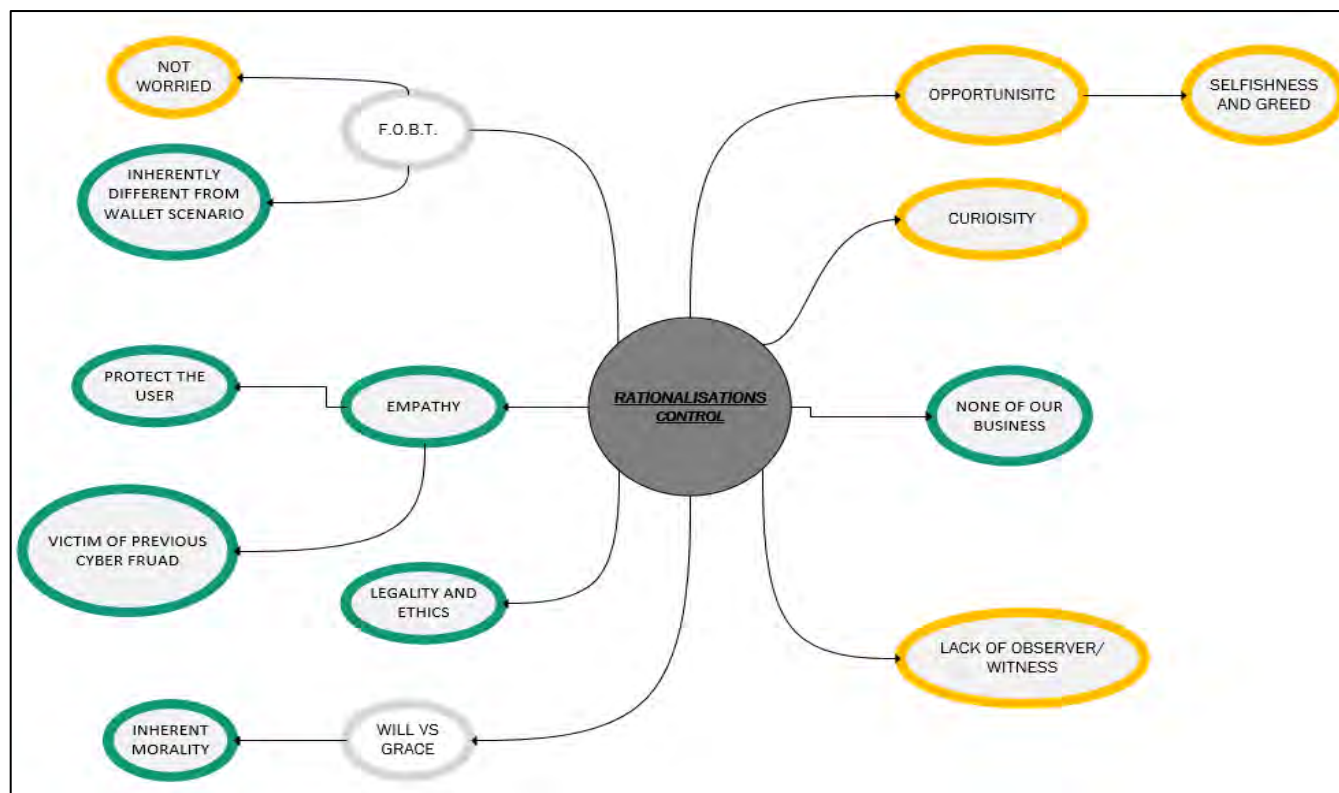


Figure D4: Initial thematic map (Control) thought process and rationalisations (no quotations: Phase 3 product)

Table D1: Control rationalisation refinement 1

| Refined theme(s) | [Original theme(s)] |
|--|--|
| Morality and social norms | [None of our business] |
| Legal and moral guidelines for behaviour | [Legality and ethics], [Will vs Grace] |
| Good Samaritan helps people in trouble | [Empathy] + children |
| Digital context of online banking (traces) | [F.O.B.T.] + children |
| Opportunity and temptation | [Lack of observer/witness], [opportunistic], [curiosity] |

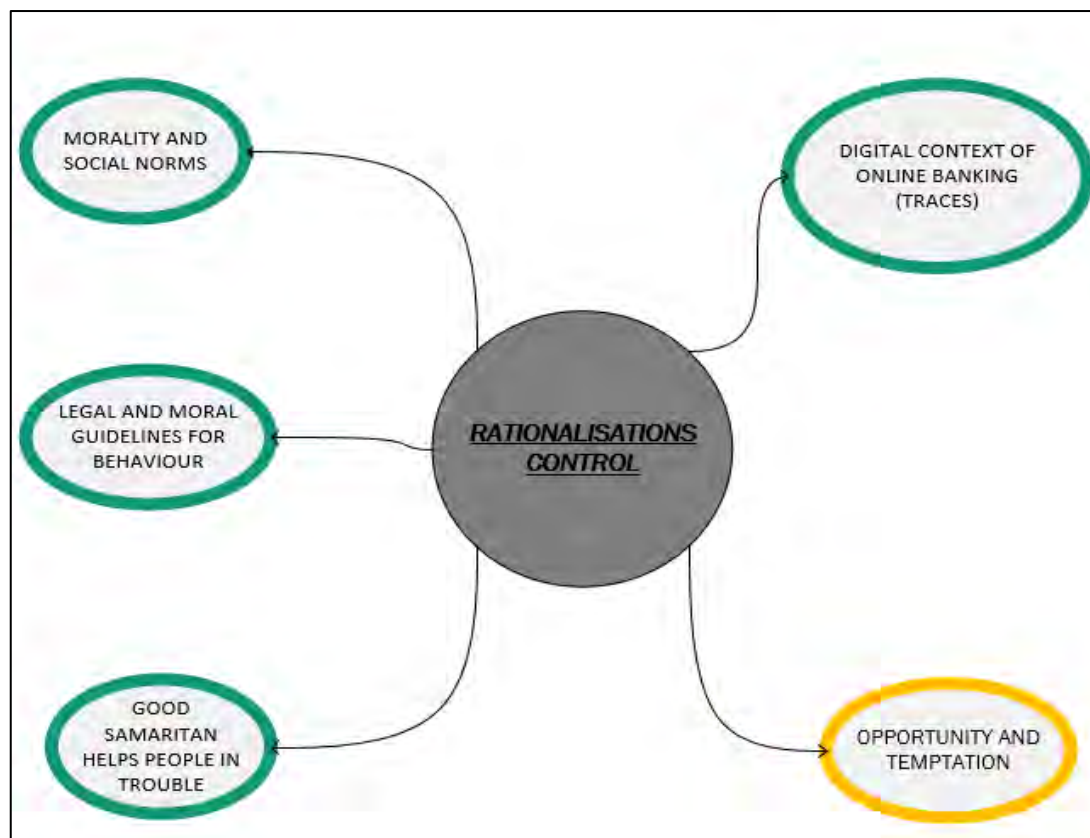


Figure D5: Control thought process and rationalisations refined V1 (Phase 4)

Table D2: Control rationalisation refinement 2

| Refined theme(s) | [Original theme(s)] |
|---|--|
| Moral and social norms encourage helping those who make mistakes | [Good Samaritan helps people in trouble], [morality and social norms] |
| Tempting opportunity in digital context comes with more risk than wallet scenario | [Digital context of online banking (traces)], [opportunity and temptation] |
| Legal restrictions and social/moral/ norms discourage dishonesty | [Legal and moral guidelines for behaviour] |

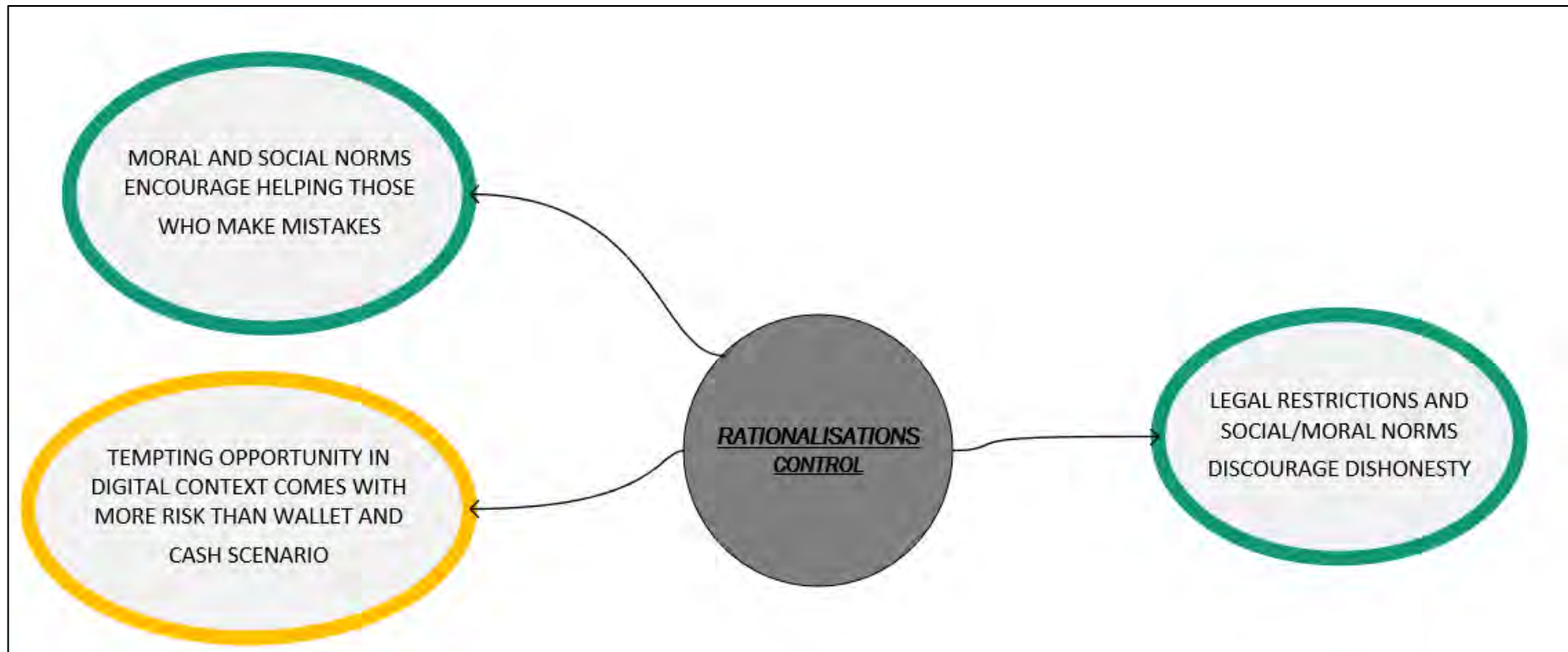


Figure D6: Control thought process and rationalisations refined V2 (Phase 4)

Table D3: Control rationalisation refinement 3

| Refined theme(s) | [Original theme(s)] |
|--|---|
| Legal restrictions, moral and social norms encourage honesty and helping others | [Legal restrictions and social/moral/ norms discourage dishonesty] + [moral and social norms encourage helping those who make mistakes] |
| Tempting opportunity in digital context comes with more risk than wallet AND cash scenario | [Tempting opportunity in digital context comes with more risk than wallet scenario] |

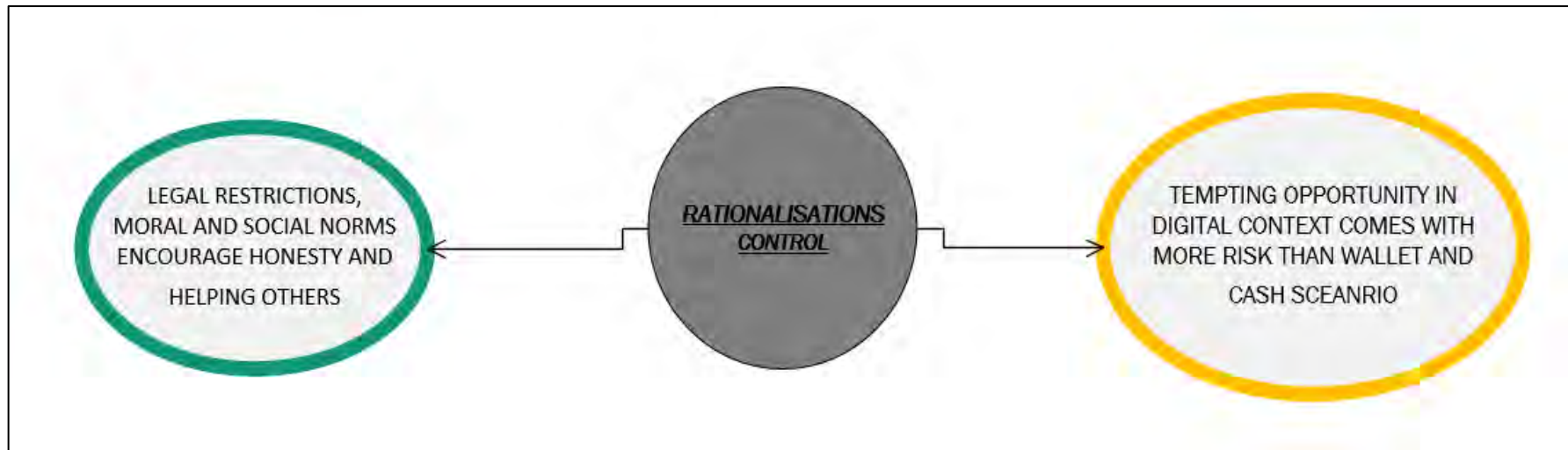


Figure D7: Control thought process and rationalisations refined V3 (Phase 4)

PRE-LOG

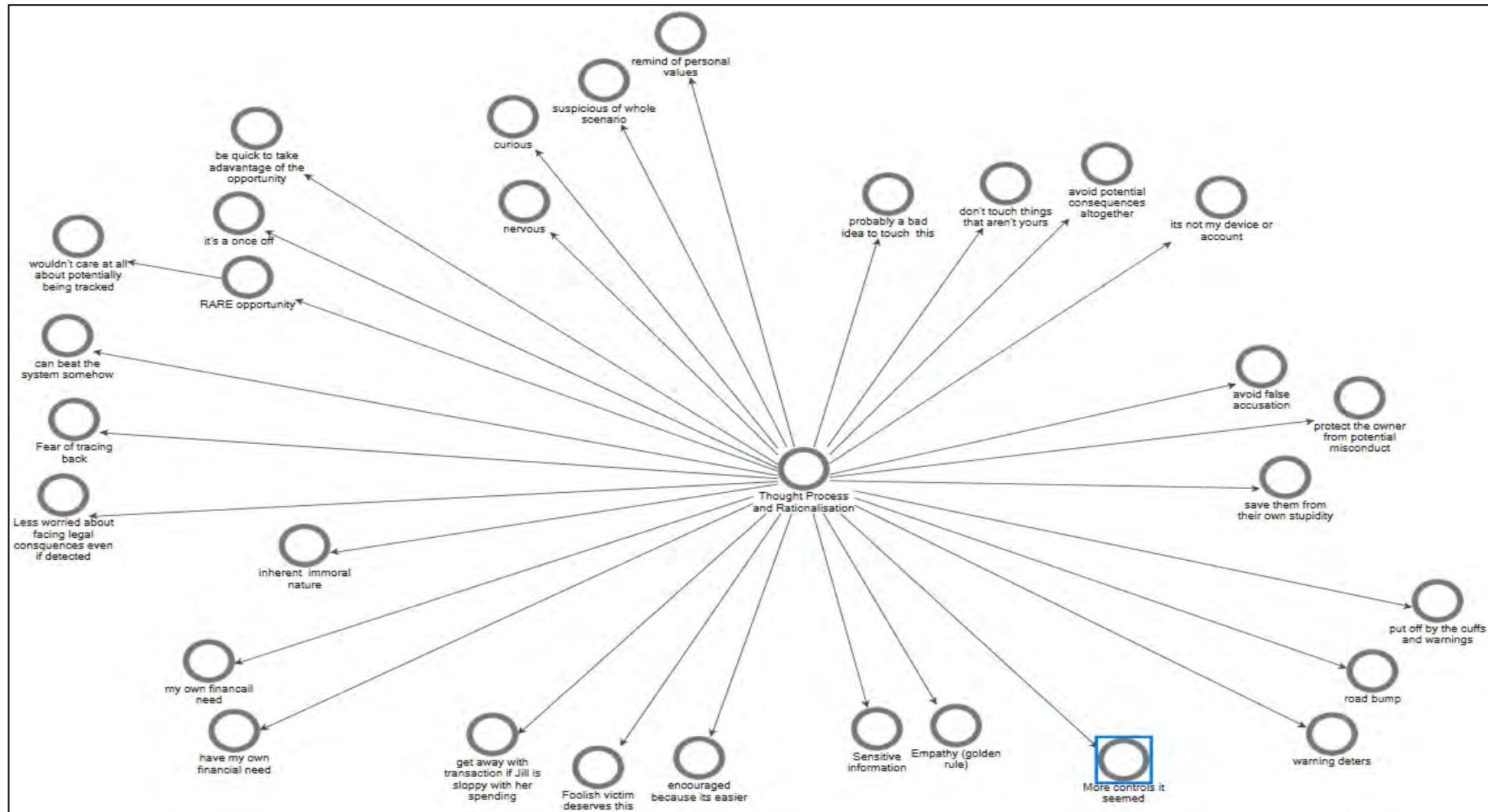


Figure D8: PRE-LOG thought process and rationalisations project map (Phase 2 of Braun and Clarke, 2006)



Figure D9: Initial thematic map: PRE-LOG thought process and rationalisations: left side (Phase 3)

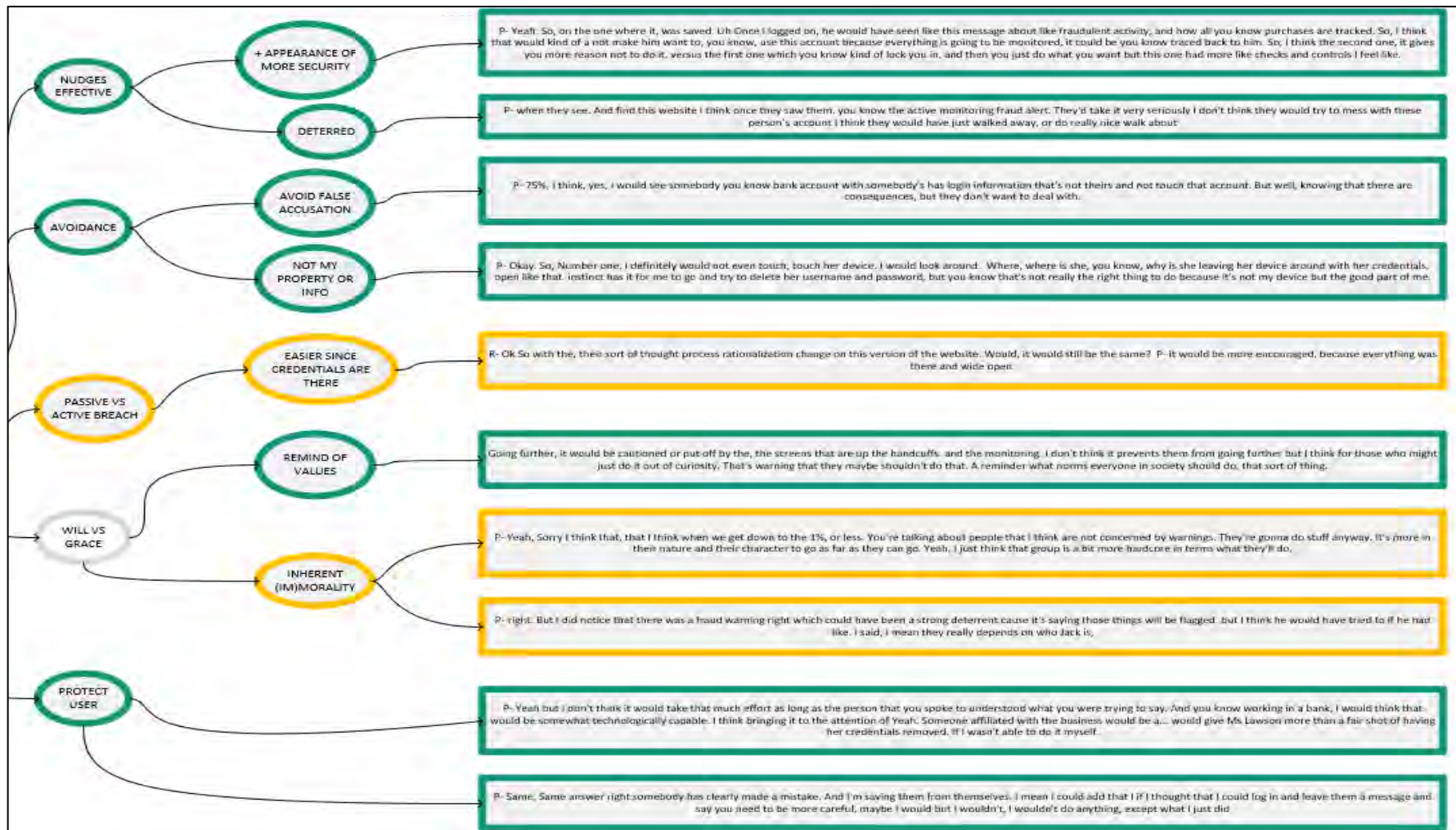


Figure D10: Initial thematic map: PRE-LOG thought process and rationalisations: right side (Phase 3)

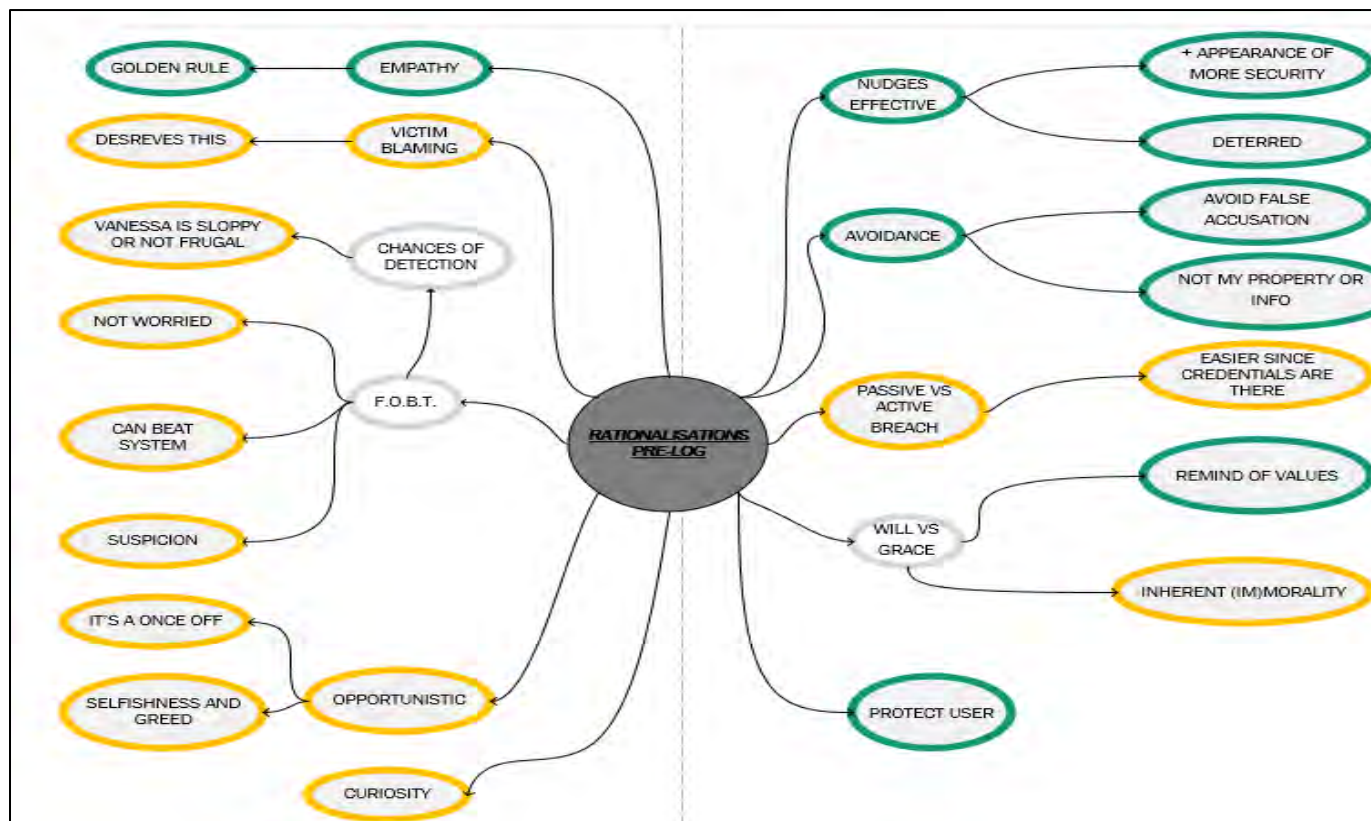


Figure D11: Initial thematic map: PRE-LOG thought process and rationalisations (no quotations) (Phase 3)

Table D4: PRE-LOG rationalisation refinement 1

| Refined theme(s) | [Original theme(s)] |
|--|---|
| Impression of higher chances of detection make people have second thoughts | [Nudges effective] + children |
| Digital context + low or acceptable risk of detection | [F.O.B.T.] + children |
| Good Samaritan does not want to hurt others (recognises mistake) | [Empathy] + child |
| Legal, moral, and social norms | [Avoidance] + children |
| Inherently dishonest people must be encouraged to be honest | [Will vs Grace] + children |
| Opportunity legitimate | [Suspicion] |
| Rare chance to enrich self | [Curiosity], [opportunistic] + children |
| Teach victim hard lesson | [Victim blaming] + child |
| I'm not so bad since I did not go looking or steal credentials | [Passive vs active breach] |

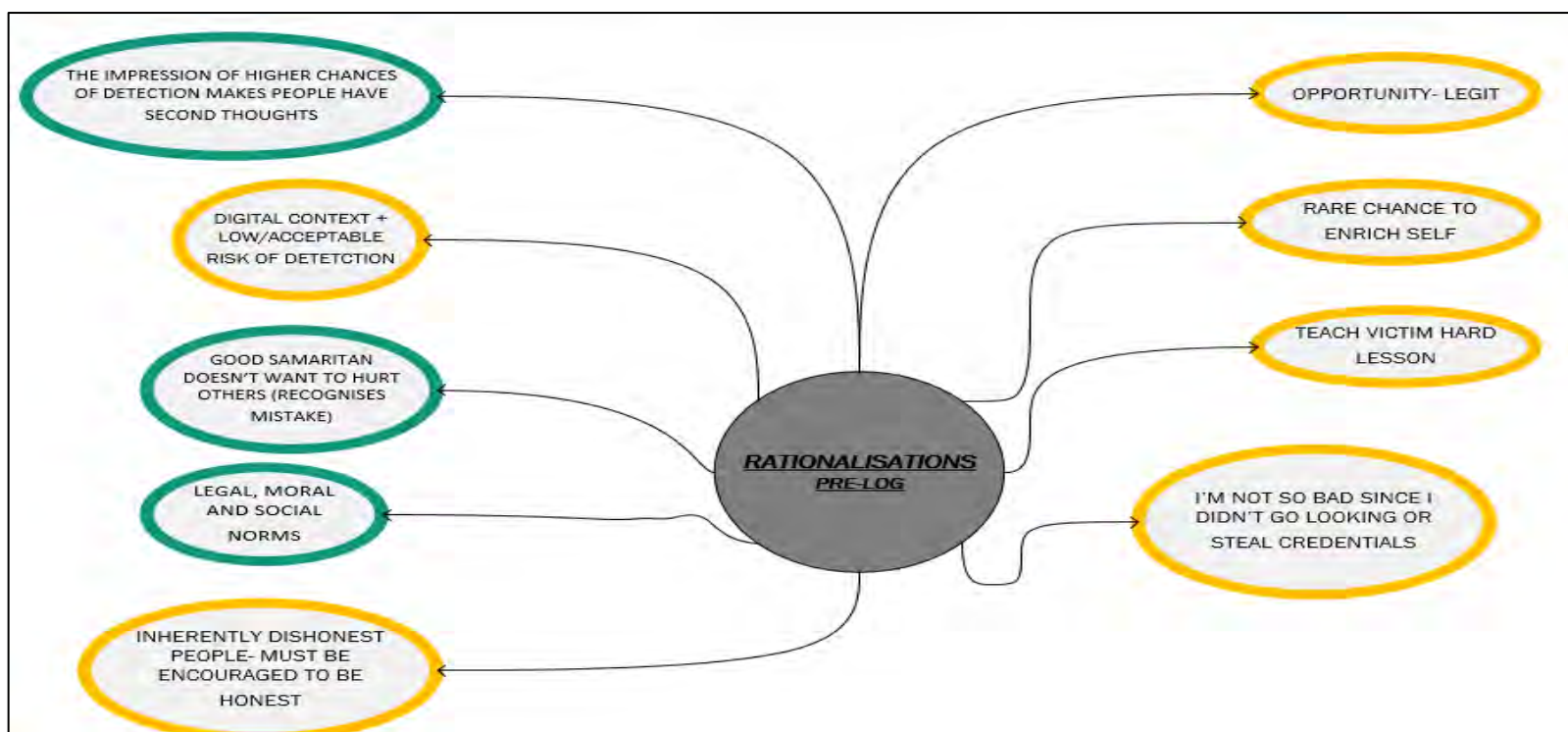


Figure D12: PRE-LOG thought process and rationalisations refined V1 (Phase 4)

Table D5: PRE-LOG rationalisation refinement 2

| Refined theme(s) | [Original theme(s)] |
|---|--|
| Hurt them because of their mistakes | [Teach victim hard lesson] |
| Moral self-concept threat reduced | [I'm not so bad since I didn't go looking or steal credentials] |
| People's inherent nature dictates response to opportunity or scenario | [Good Samaritan doesn't want to hurt others (recognises mistake)], [inherently dishonest people must be encouraged to be honest] |
| Digital context and perception of risk (chances of detection) | [Impression of higher chances of detection make people have second thoughts] |
| Possible opportunity to enrich self | [Rare chance to enrich self], [opportunity legit?] |
| Legal restrictions + moral & social norms encourage honesty | [Good Samaritan doesn't want to hurt others (recognises mistake)], [legal, moral, social norms] |

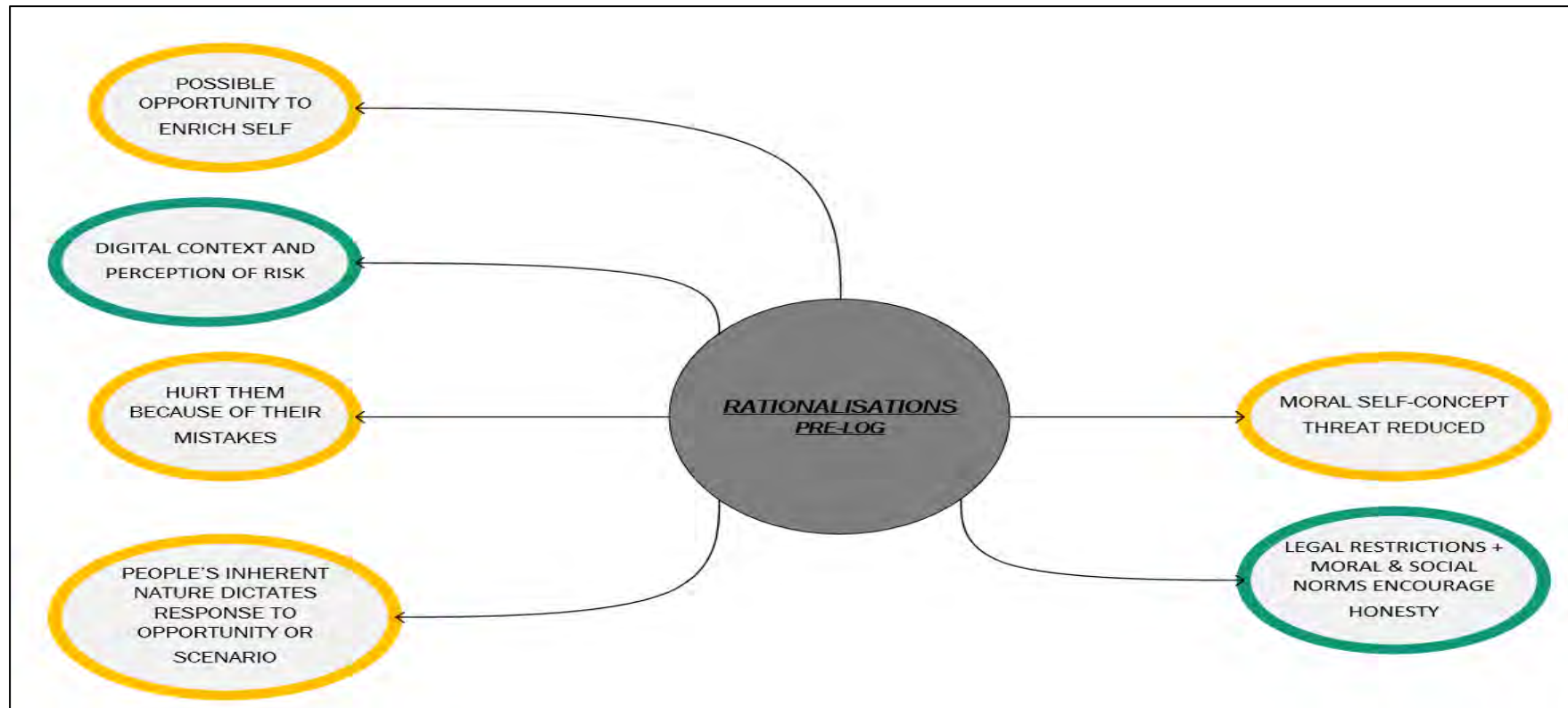


Figure D13: PRE-LOG thought process and rationalisations refined V2 (Phase 4)

Table D6: PRE-LOG rationalisation refinement 3

| Refined theme(s) | [Original theme(s)] |
|--|---|
| Inherent nature and importance of moral self-concept | [People's inherent nature dictates response to opportunity or scenario] |
| Digital context and perception of risk | [Possible opportunity to enrich self], [digital context and perception of risk] |
| Hurt them because of their mistakes | |

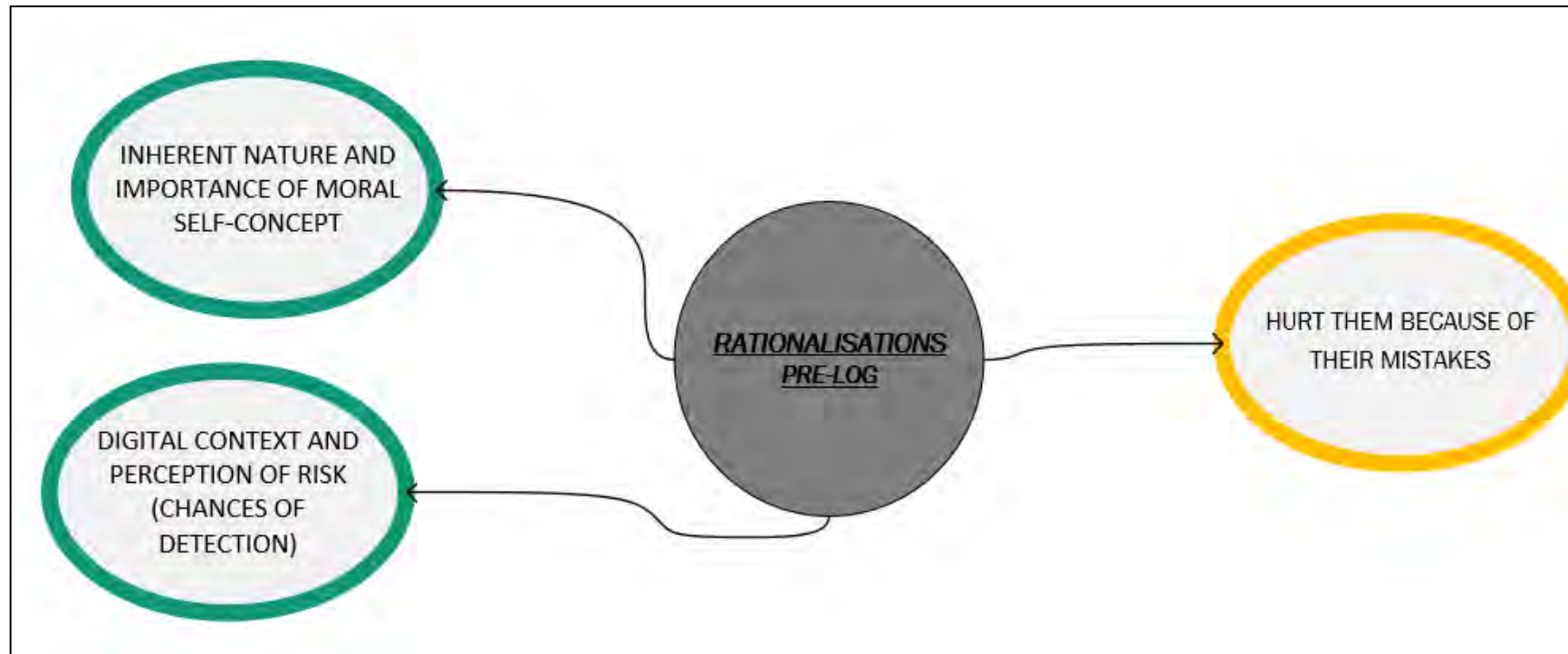


Figure D14: PRE-LOG thought process and rationalisations refined V3 (Phase 4)

POST-LOG

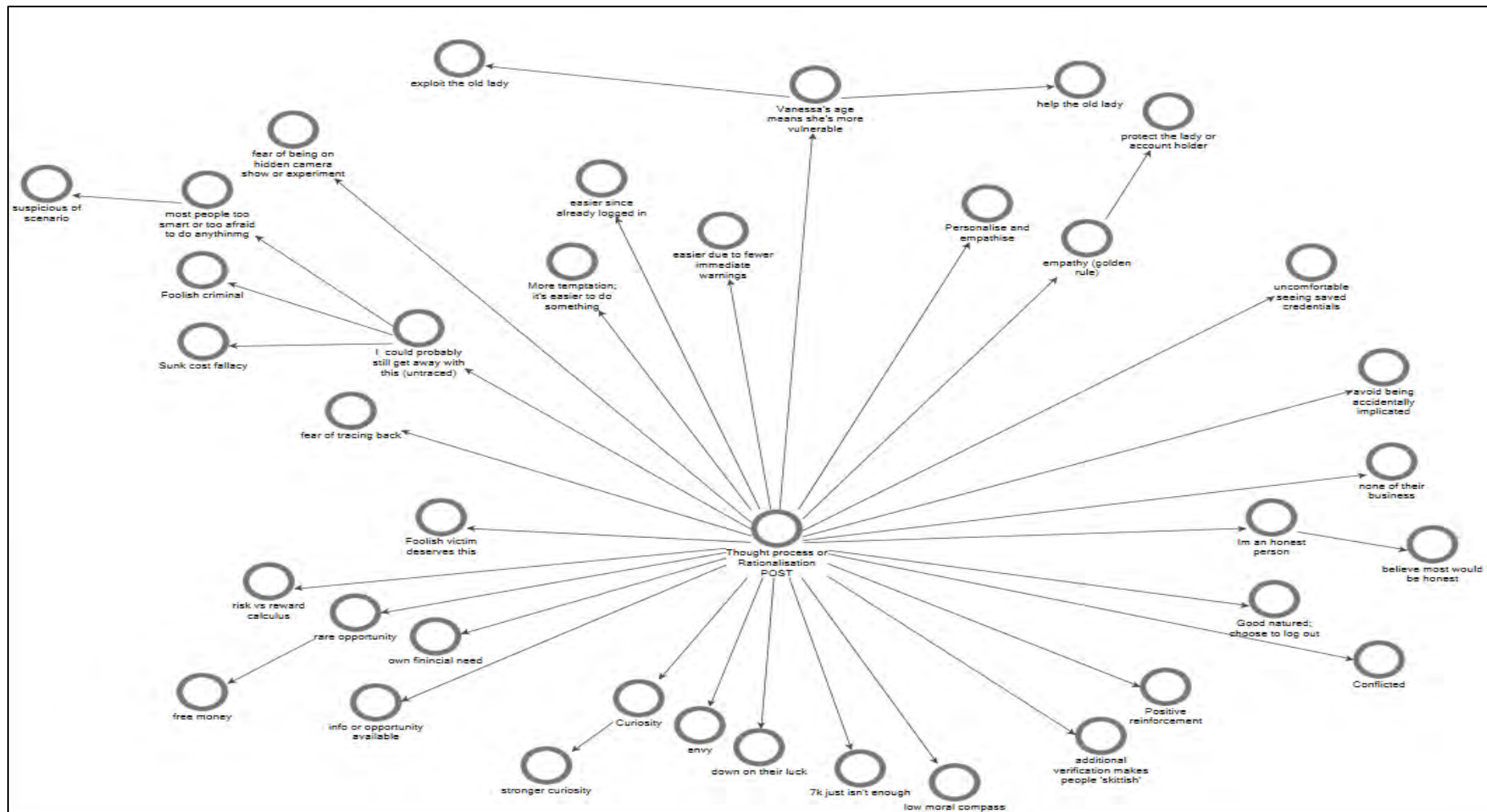


Figure D15: POST-LOG thought process and rationalisations project map (Phase 2 of Braun and Clarke, 2006)



Figure D16: Initial thematic map POST-LOG thought process and rationalisations: left side (Phase 3)

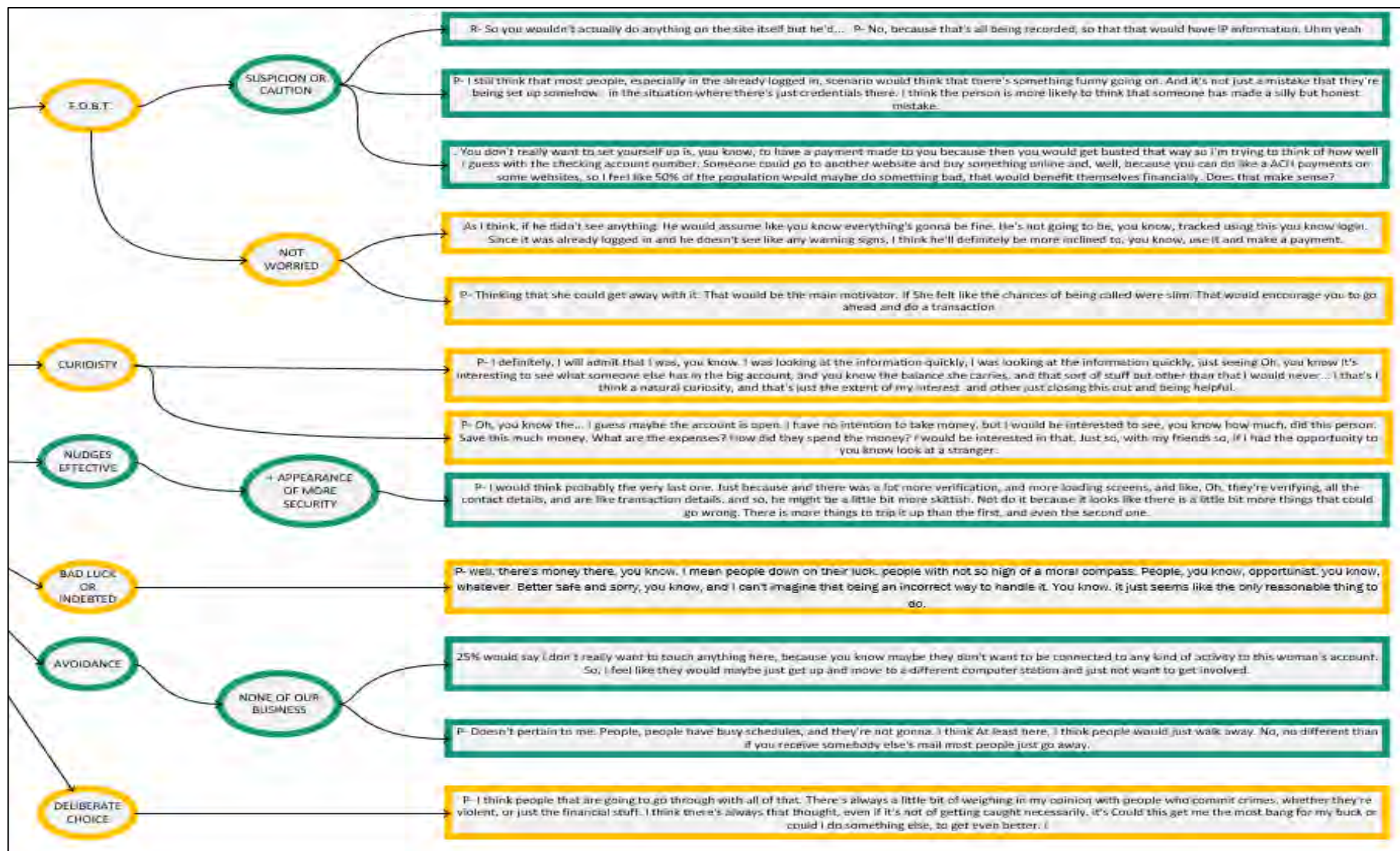


Figure D17: Initial thematic map POST-LOG thought process and rationalisations: right side (Phase 3)

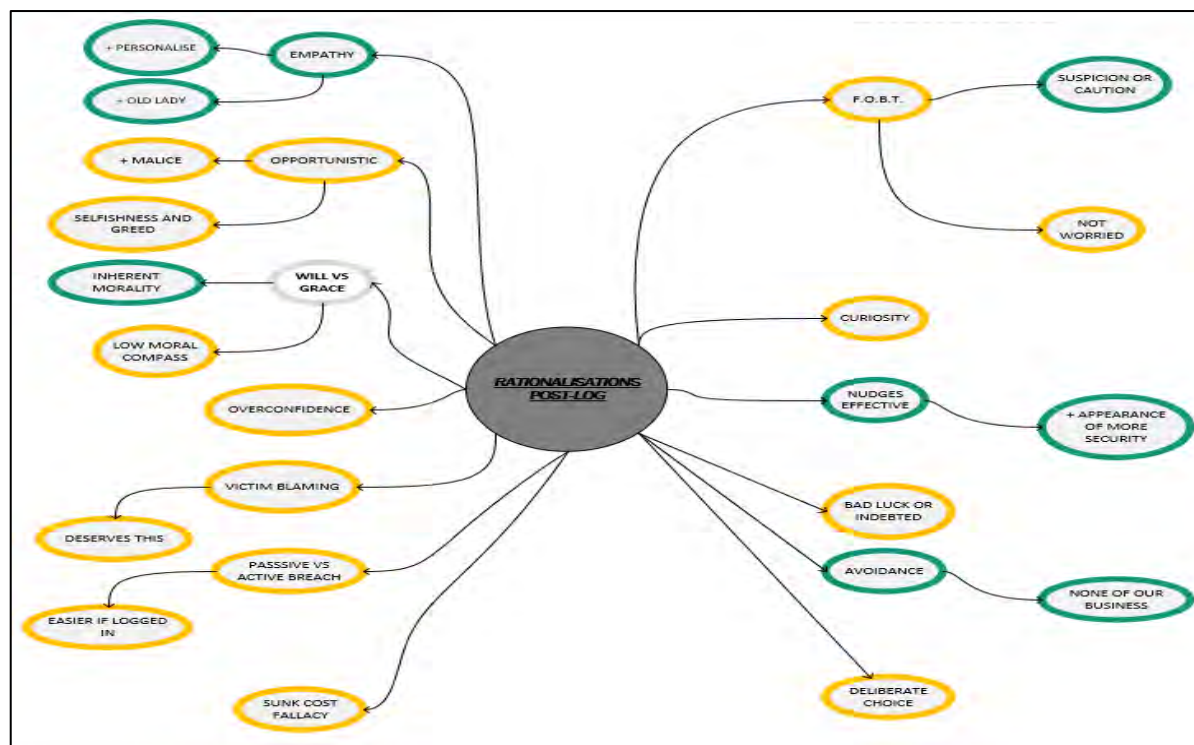


Figure D18: Initial thematic map (POST-LOG) thought process and rationalisations: no quotations (Phase 3 product)

Table D7: POST-LOG rationalisation refinement 1

| Refined theme(s) | [Original theme(s)] |
|--|---------------------------------------|
| Can better picture victim | [Empathy] + children |
| Opportunity to enrich self | [Selfishness and greed] |
| Teach victim a hard lesson | [Deserves this] + [malice] |
| I'm not so bad because I didn't actively compromise the account myself | [Passive vs active breach] + children |
| Low or acceptable chances of detection | [Not worried] + [overconfidence] |
| Social norms – don't get involved | [Avoidance] + children |
| Some people, by nature, are dishonest/honest | [Will vs Grace] + children |
| Perception of higher security (chances of detection) | [Nudges effective] + children |
| Opportunity and temptation + biased/ flawed logic | [Sunk cost fallacy] + [curiosity] |
| Opportunity legit | [Suspicion or caution] |

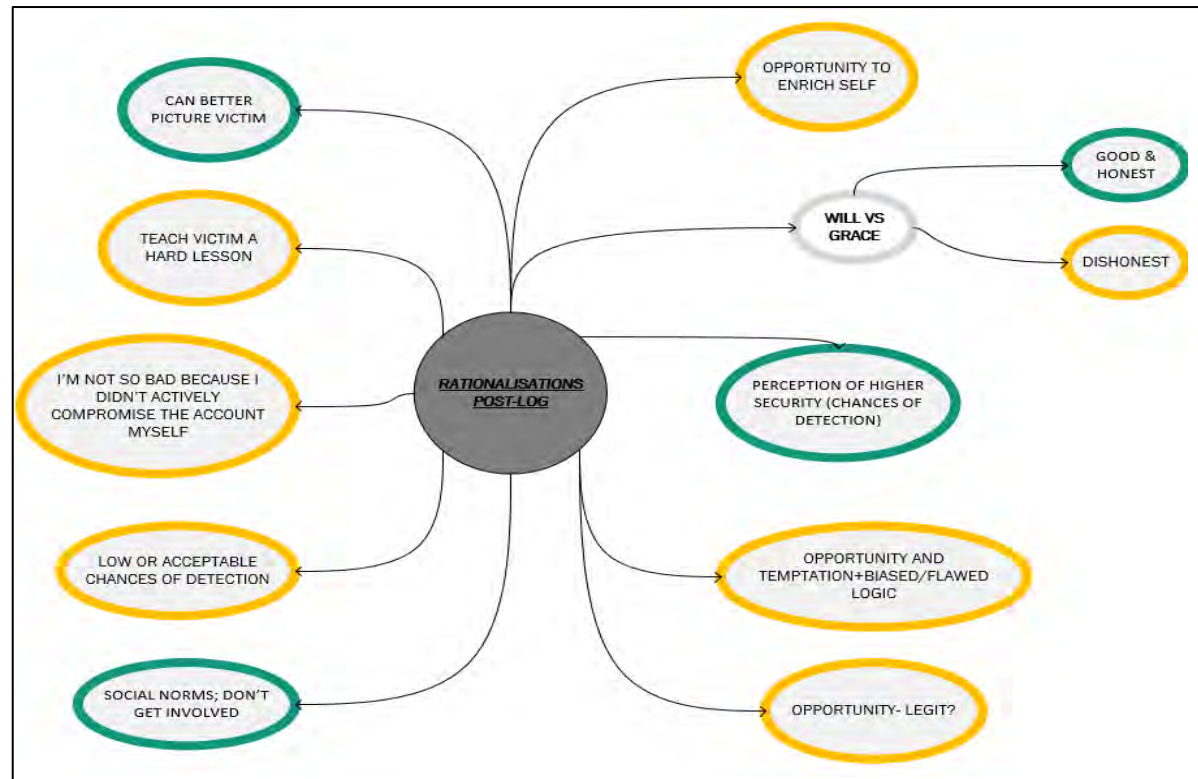


Figure D19: POST-LOG thought process and rationalisations refined V1 (Phase 4)

Table D8: POST-LOG rationalisation refinement 2

| Refined theme(s) | [Original theme(s)] |
|---|---|
| Hurt them because of their mistakes | [Teach victim a hard lesson] |
| Perception of higher chances of detection | [Low or acceptable chances of detection] + [perception of higher security (chances of Detection)] |
| People's inherent nature dictates response to opportunity or scenario | [Opportunity to enrich self] + [some people by nature are dishonest/honest] |
| Harming a real person is much harder | [Can better picture victim] |
| Moral self-concept threat reduced | [I'm not so bad because I didn't actively compromise the account myself] |
| Justify exploiting fraud opportunity with biased logic | [Opportunity to enrich self] + [opportunity legit] |

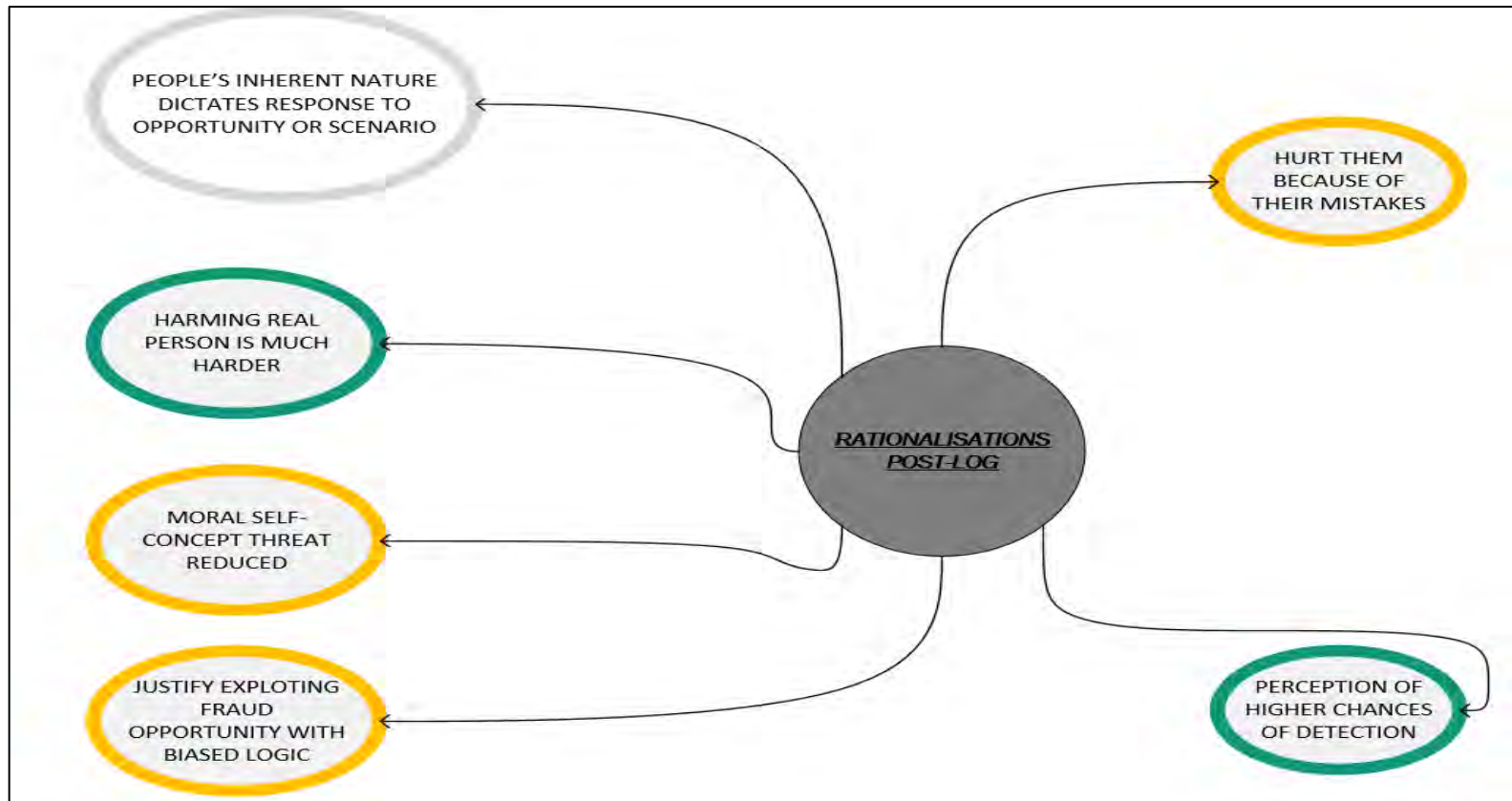


Figure D20: POST-LOG thought process and rationalisations refined V2 (Phase 4)

Table D9: POST-LOG rationalisation refinement 3

| Refined theme(s) | [Original theme(s)] |
|--|--|
| Justifying fraud using biased or selfish logic | [Moral self-concept threat reduced] + [justify exploiting fraud opportunity with biased logic] + [hurt them because of their mistakes] |
| Inherent nature and Importance of honest or moral self-concept | [People's inherent nature dictates response to opportunity or scenario] + [harming real person is much harder] + [moral self-concept threat reduced] |
| Perception of higher chances of detection | |

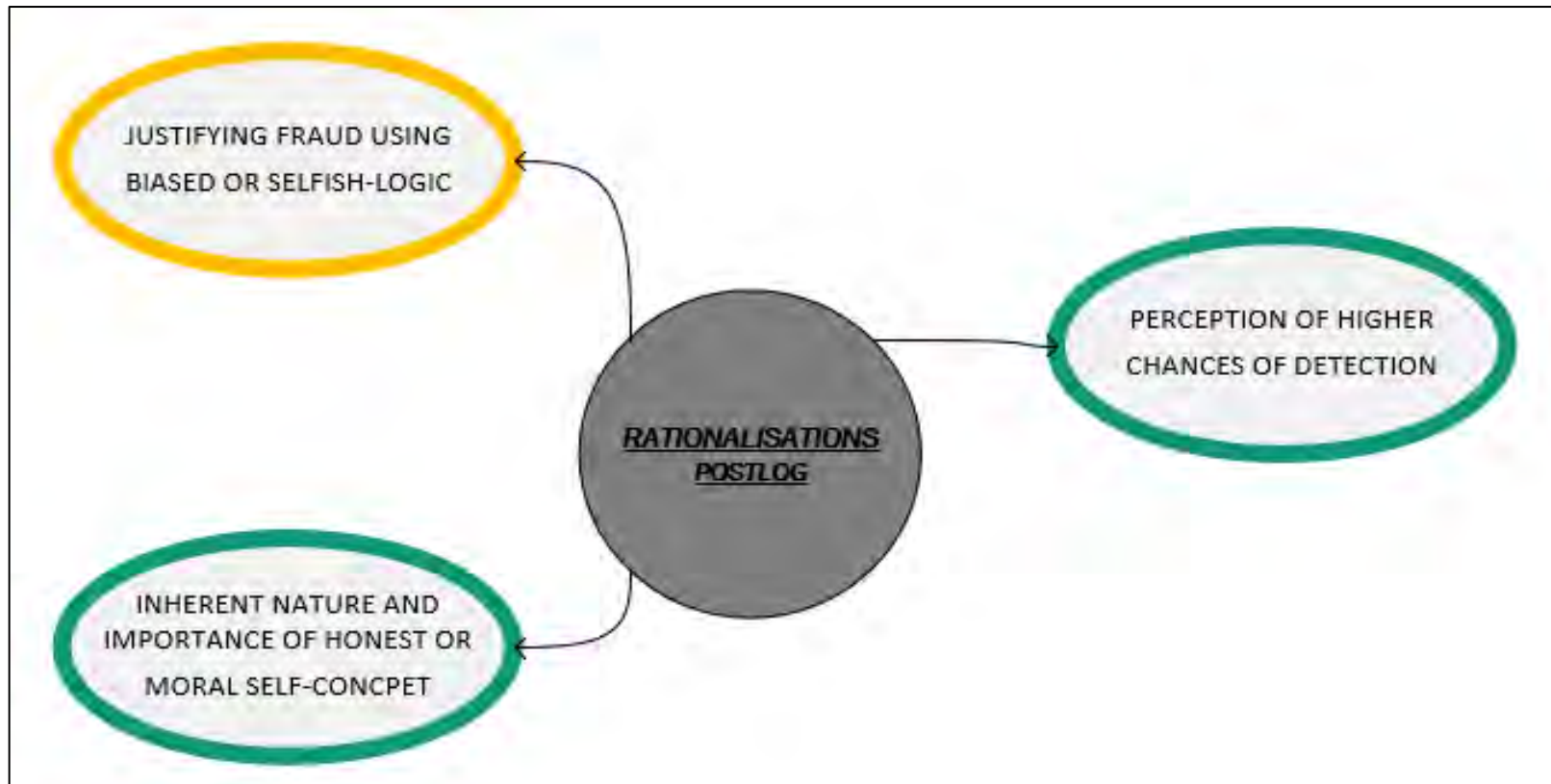


Figure D21: POST-LOG thought process and rationalisations refined V3 (Phase 4)

APPENDIX E: MISCELLANEOUS

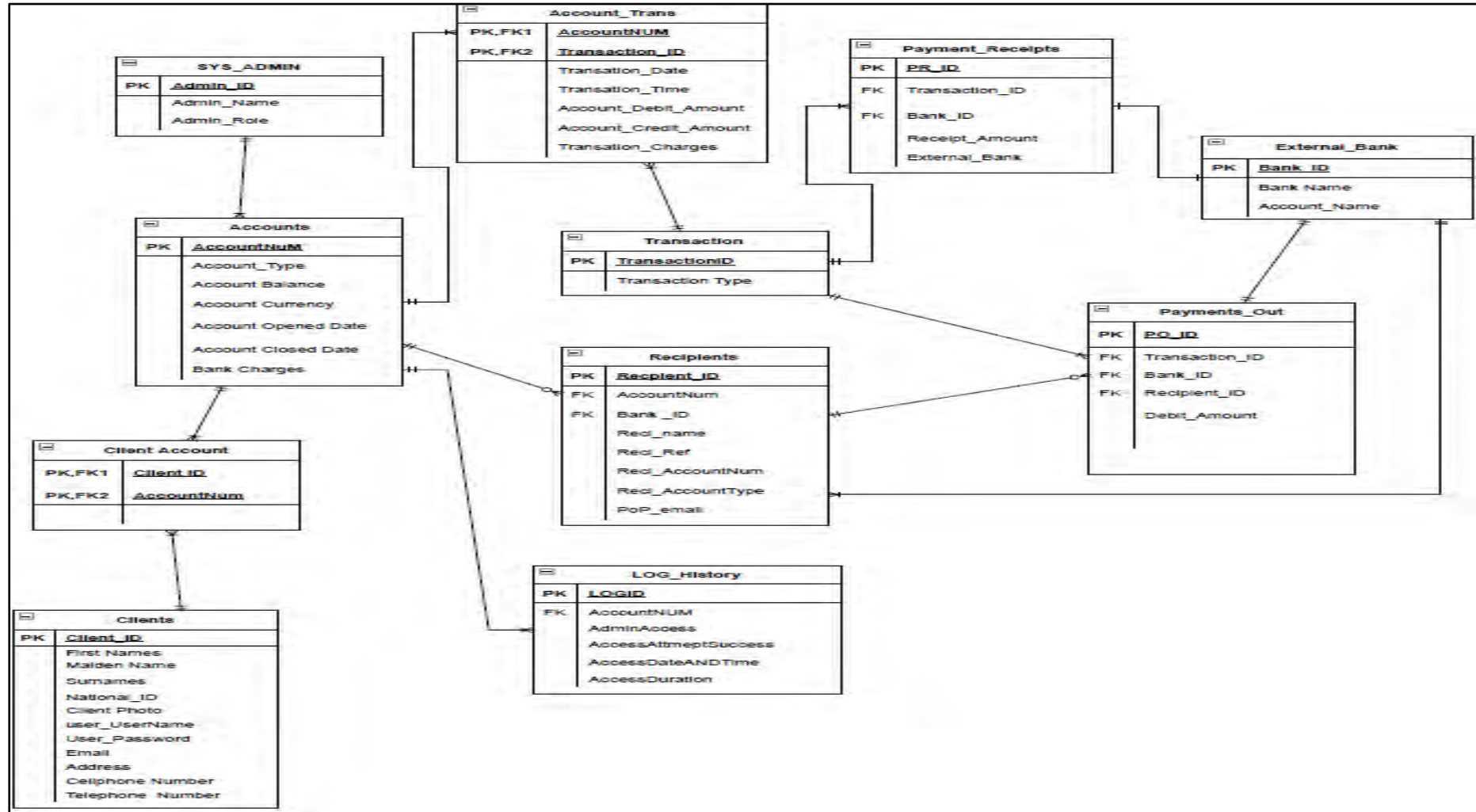


Figure E1: Entity Relationships Diagram (ERD) of limited online banking system

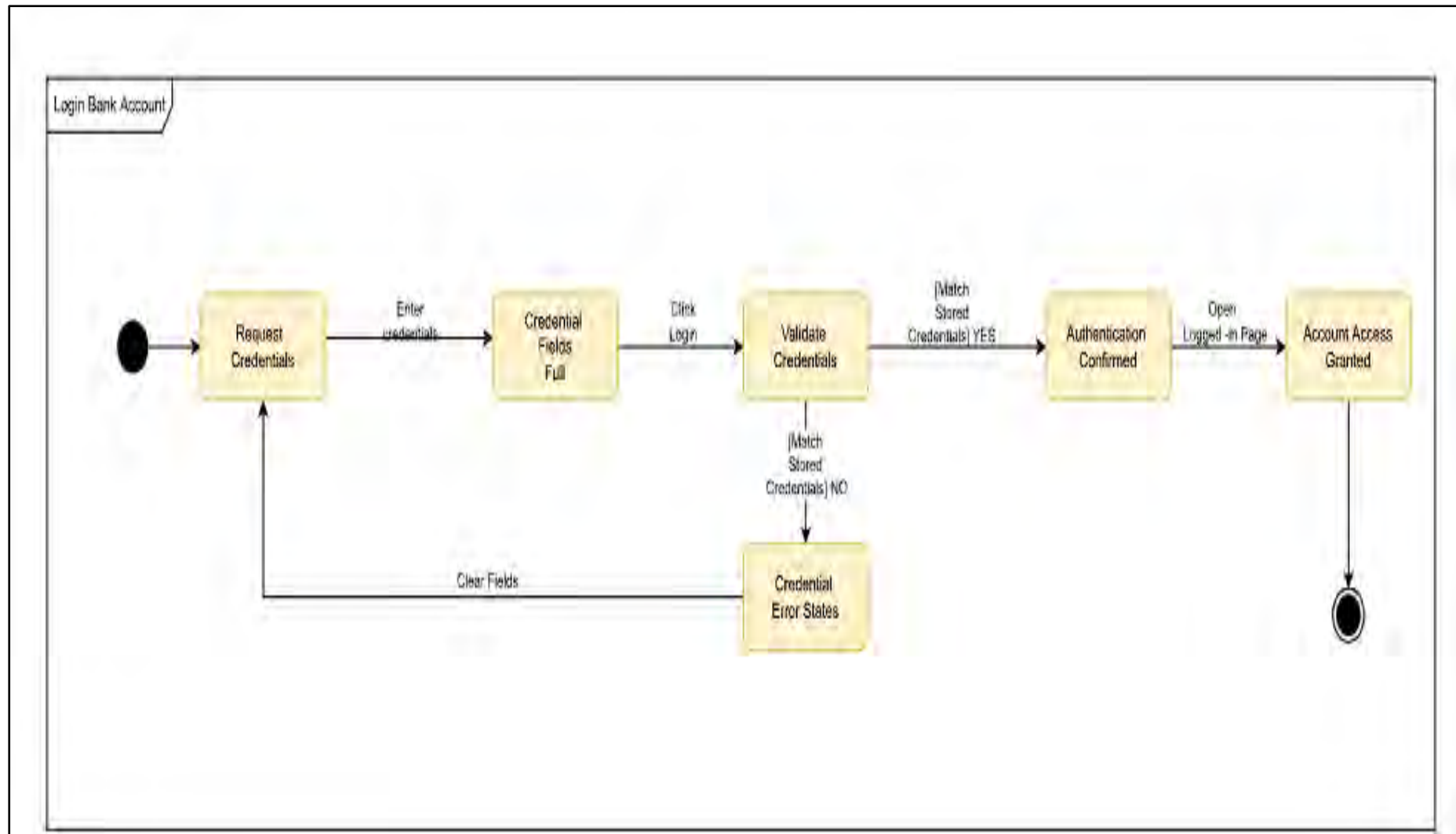


Figure E2: Behavioural state machine: Login

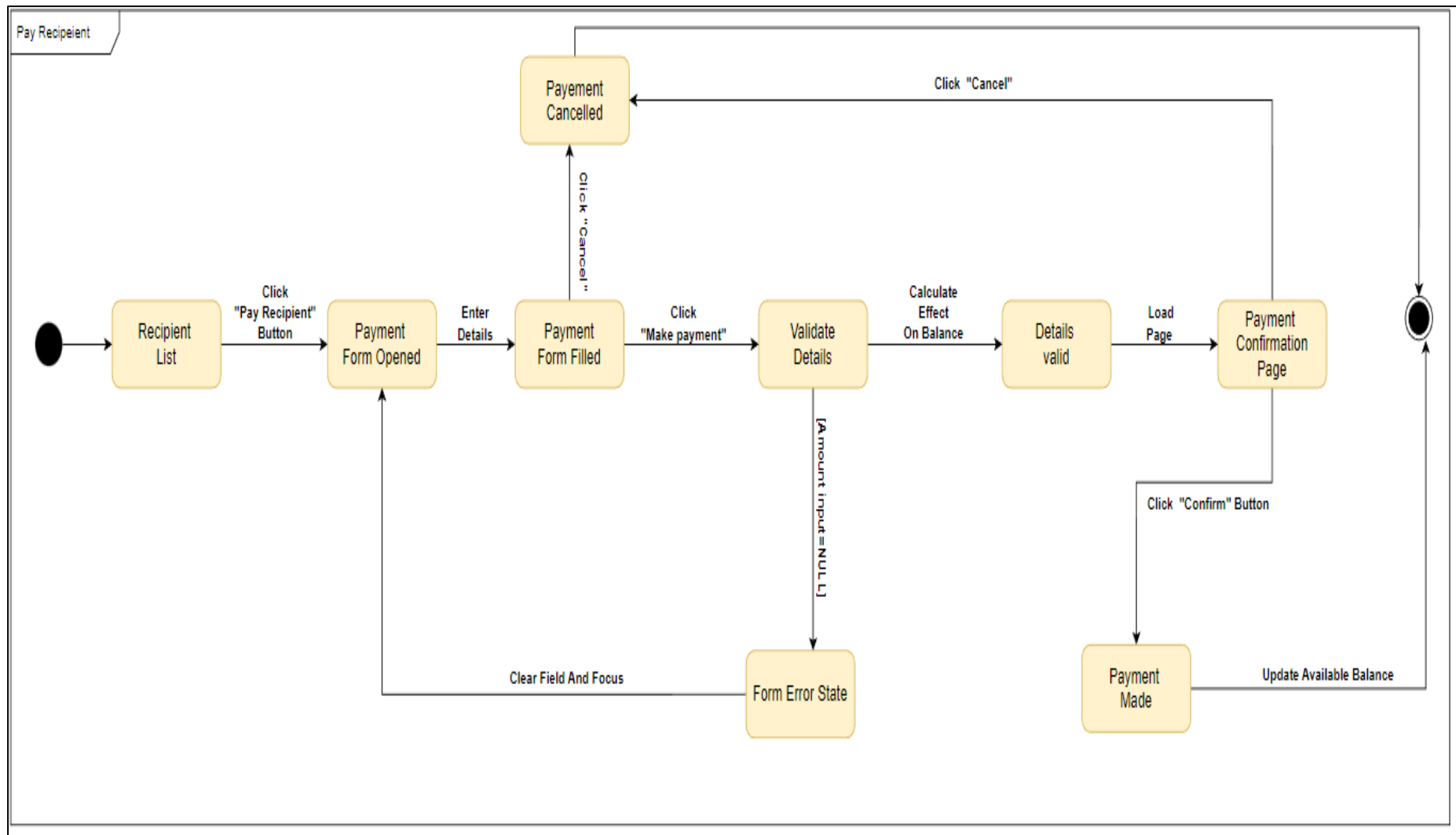


Figure E3: Behavioural state machine: Payment

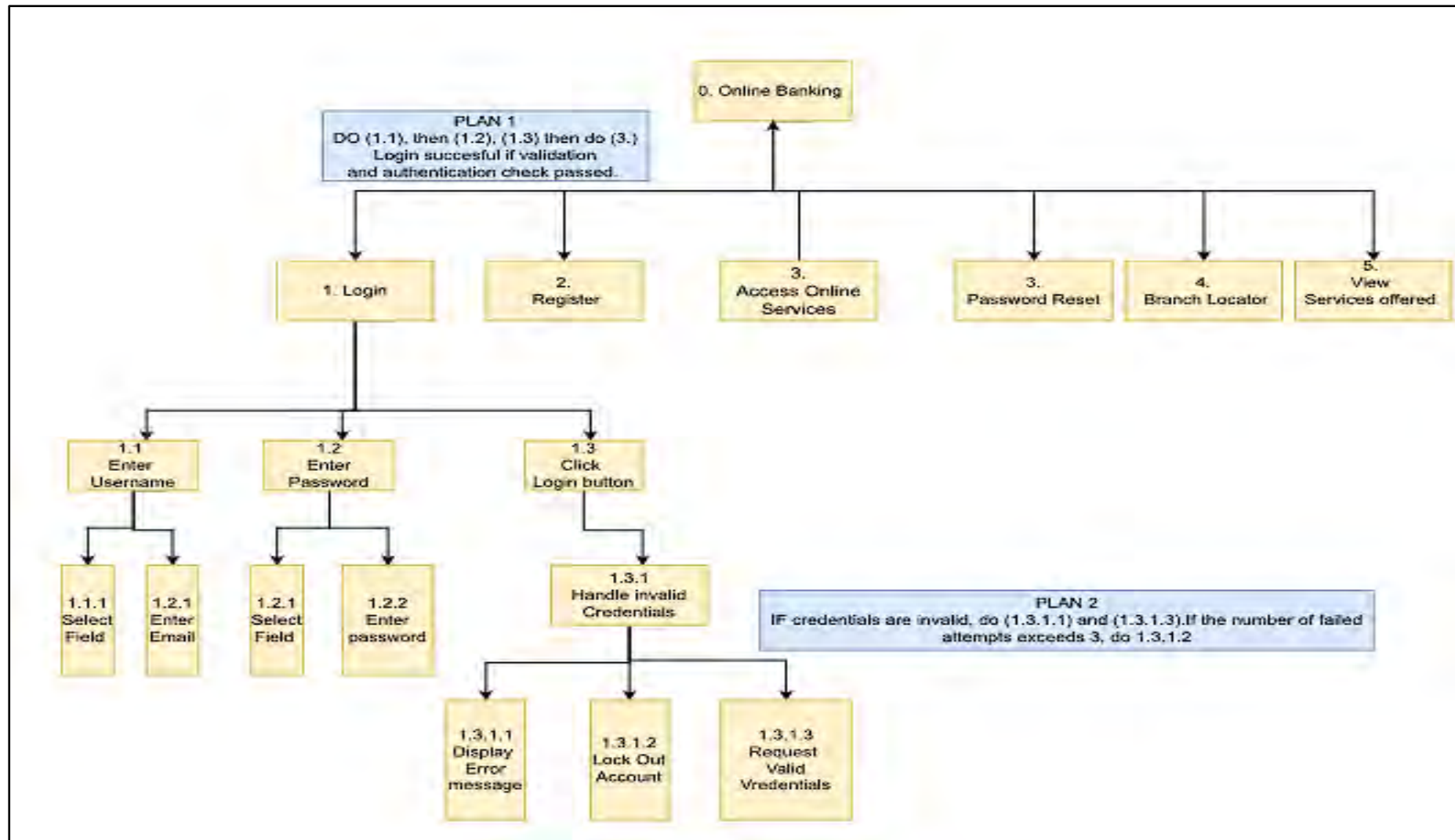


Figure E4: Hierarchical task analysis (HTA): Online banking website

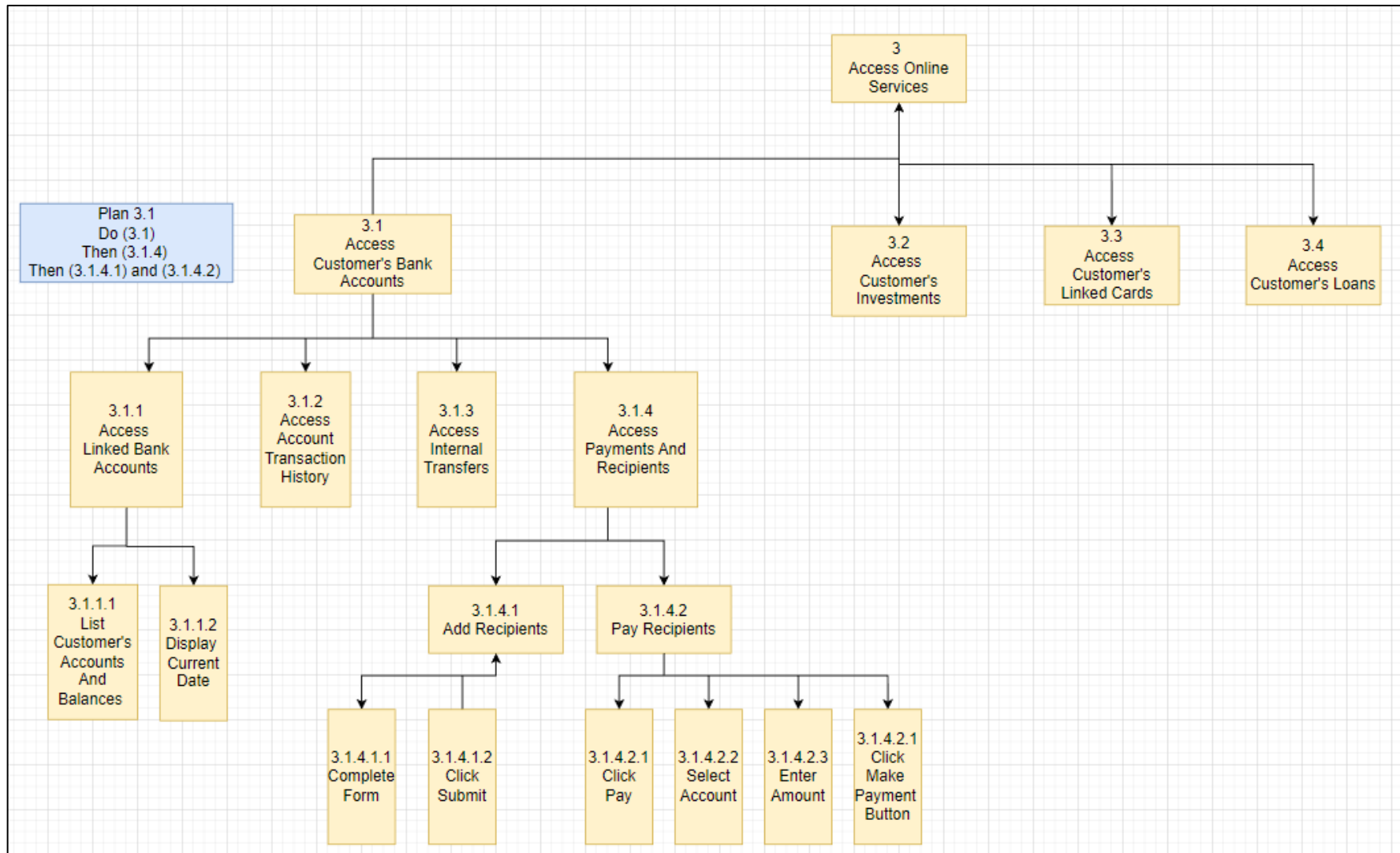


Figure E5: HTA: Access services (payments)