Identification and Prevention of Banking Fraud and Scams in New Zealand

Evgenii Babenkov
Student ID number: 1000097549

The Research Thesis is submitted in the achievement of the degree Master of Applied Management at Otago Polytechnic Auckland International Campus, New Zealand.

December 2021
Declaration Concerning Thesis Presented for the Degree of Master of Applied Management

I, Evgenii Babenkov, of Auckland, New Zealand, solemnly and sincerely declare, in relation to the Thesis entitled:

Identification and Prevention of Banking Fraud and Scams in New Zealand

(a) That work was done by me, personally

and

(b) The material has not previously been accepted in whole, or in part, for any other degree or diploma

Signature:

Date: 25 December 2021
Abstract

Over the past few years, the finance industry has made an enormous breakthrough in applying information technology to achieve business goals. It is now impossible to imagine any financial institute operating without modern electronic technology. However, the development of information technologies in banking and their introduction into all aspects of financial life has led to the emergence of a new type of crime – banking fraud and scams. Fraud and scams are a universal phenomenon that have existed since historical times and is one of the major enemies of the business world. Fraud and scams exist in all walks of life, government, banking, export/import sectors, shipping, insurance, real estate, and more. Nowadays, fraud and scams in the banking sector is the most significant problem, as it directly impacts the health and prosperity of the global economy and individual countries. The magnitude of bank fraud cannot be known because much of it is undisclosed or undetected, and not all that is discovered is published.

The key aim of this research is to investigate banking fraud in New Zealand and create a simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud or scams. In addition, the research will help to understand technical aspects and types of bank fraud and scams committed via banking card and online-banking in New Zealand. Moreover, the research will examine the New Zealand governments' and financial institutions' response in the prevention and control of bank fraud, including what actions have been completed until now and what else the New Zealand government can do.

A mixed methodology was used to conduct this research which involved face-to-face interviews with banking industry professionals and online questionnaires with the users of banking services. Descriptive and inferential statistics were used for the quantitative analysis of the data. A qualitative method was used to build the hypotheses and draw conclusions by triangulating information acquired from research participants and the review of open information sources published worldwide.

The research involved 113 banking services users and five financial industry professional experts from the financial and cybersecurity industry. Interaction with the online questionnaire research participants took place through the professional social media platform LinkedIn. The face-to-face interviews were conducted online via Microsoft Teams.

This research was able to provide answers to the three research questions crafted in this Thesis. The most common types of banking fraud and scams were identified by surveying banking services users, some of whom are victims of fraud and by interviewing financial industry professional experts
from the financial and cybersecurity industry then comparing the opinions of the two groups. The involvement of the New Zealand government and financial institutions in the combat against fraud was also analysed. This analysis was based on banking services users’ personal opinions, professional opinions of the financial industry professional experts, and information found from official sources. Based on the research insights, expert opinion, and the world's best practices, the research proposed measures to strengthen the mitigating of risk of fraud and developed a set of rules to avoid fraud.

Although this research had several limitations due to the problematic situation worldwide and New Zealand, research methods and approaches did not prevent the completion of this research. In addition, the limitations described above open prerequisites for future researchers.
Acknowledgements

Firstly, I would like to say a big “thank you” to my family for supporting me throughout this research and during these challenging times.

I express my appreciation to Dr. Farhad Mehdipour, my research supervisor, and Saba Saimei, my research co-supervisor. Our meetings, discussions, and brainstorming were priceless for me and my research.

My acknowledgements to Dr. Indrapriya Kularatne for providing the opportunity to become a part of the research community and general support.

My gratefulness to Otago Polytechnic Auckland International Campus, for the generous student support and the vast range of different student events.

My huge appreciation for New Zealand, the country that accepted my presence and provided me with a chance to achieve my goals.

My acknowledgements to the anonymous research participants and financial industry professional experts who provided their opinions and shared the experience.

Finally, I would like to credit to my friends, whose support I was feeling all the time.
### Table of contents

**Chapter I: Introduction**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Introduction</td>
<td>9</td>
</tr>
<tr>
<td>1.2 Background</td>
<td>10</td>
</tr>
<tr>
<td>1.2.1 Overview of the New Zealand financial and banking industry</td>
<td>10</td>
</tr>
<tr>
<td>1.2.2 Concept of fraud and scam</td>
<td>13</td>
</tr>
<tr>
<td>1.2.3 Theoretical framework of fraud</td>
<td>15</td>
</tr>
<tr>
<td>1.3 Research aims, questions, and significance</td>
<td>18</td>
</tr>
<tr>
<td>1.4 Research process and phases</td>
<td>19</td>
</tr>
<tr>
<td>1.5 Chapter summary</td>
<td>22</td>
</tr>
</tbody>
</table>

**Chapter II: Literature review**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Introduction</td>
<td>23</td>
</tr>
<tr>
<td>2.2 Banking fraud and scam</td>
<td>23</td>
</tr>
<tr>
<td>2.2.1 General meaning of banking fraud</td>
<td>23</td>
</tr>
<tr>
<td>2.2.2 Causes of banking fraud</td>
<td>24</td>
</tr>
<tr>
<td>2.2.2.1 Institutional Factors</td>
<td>25</td>
</tr>
<tr>
<td>2.2.2.2 External/Environmental Factors</td>
<td>26</td>
</tr>
<tr>
<td>2.2.3 Types of banking fraud</td>
<td>26</td>
</tr>
<tr>
<td>2.2.3.1 Internet fraud</td>
<td>27</td>
</tr>
<tr>
<td>2.2.3.1.1 Phishing</td>
<td>27</td>
</tr>
<tr>
<td>2.2.3.1.2 Pharming</td>
<td>28</td>
</tr>
<tr>
<td>2.2.3.1.3 Carding</td>
<td>29</td>
</tr>
<tr>
<td>2.2.3.2 Card fraud</td>
<td>30</td>
</tr>
<tr>
<td>2.2.3.2.1 Skimming</td>
<td>31</td>
</tr>
<tr>
<td>2.2.3.2.2 Shimming</td>
<td>33</td>
</tr>
<tr>
<td>2.2.3.2.3 Trapping</td>
<td>35</td>
</tr>
<tr>
<td>2.2.4 What is scam?</td>
<td>36</td>
</tr>
<tr>
<td>2.2.4.1 Investment scam</td>
<td>37</td>
</tr>
<tr>
<td>2.2.4.2 Romance scam</td>
<td>38</td>
</tr>
<tr>
<td>2.2.4.3 Phone scam</td>
<td>40</td>
</tr>
<tr>
<td>2.2.4.4 Other scams</td>
<td>42</td>
</tr>
</tbody>
</table>
2.3 The government’s agencies and financial institutions role
   2.3.1 Financial institutions
     2.3.1.1 Fraud identification and detection
     2.3.1.2 Fraud prevention
   2.3.2 Federal banks
   2.3. Law enforcement
2.4 Chapter II summary

Chapter III: Research Method
3.1 Introduction
3.2 Research questions
3.3 Research design
3.4 Research paradigm
3.5 Research methodology
3.6 Data collections tools
3.7 Research participants and recruitment
3.8 Data collection
3.9 Data analysis
3.10 Ethical considerations
3.11 Chapter summary

Chapter IV: Analysis
4.1 Introduction
4.2 Datasets
4.3 Data pre-processing
4.4 Descriptive analysis
   4.4.1 Customer’s and experts banking experience
   4.4.2 Familiarity and knowledge about fraud and scam
     4.4.2.1 Familiarity
     4.4.2.2 Fraud and scam typology knowledge
   4.4.3 Fraud attempts and victims
   4.4.4 Government and financial institutions involvement
     4.4.4.1 Victims support from government and banks
     4.4.4.2 Opinions about government and banks involvement
       4.4.4.2.1 Banks involvement
CHAPTER I: INTRODUCTION

1.1 Introduction

Chapter I discusses and establishes a stable theoretical foundation of banking fraud and scams, accordingly set up the goals of the research, and shows the seriousness and significance of this in New Zealand.

The following sections of Chapter I will provide financial and banking industry statistics, a historical overview, and a theoretical framework of banking fraud and scams that will help identify the gaps and emphasise the aims of the research by formulating research questions. Moreover, this chapter will describe the research process used to achieve the research goals.

Over the past few years, the finance industry has made an enormous breakthrough in applying information technology to achieve business goals. It is now impossible to imagine that any financial institute could operate without modern electronic technology (Mason, & Bohm, 2017). The role of technology is to improve citizens' lives and simplify business transactions (Airehrou, Vasudevan & Madanianet al., 2018). However, the development of information technologies in banking and their introduction into all aspects of financial life has led to the emergence of a new type of crime – banking fraud, and the way to deceive people to achieve the goals of fraud - scam (Hussaini et al., Bakar, & Yusuf, 2019).

Surprisingly, despite the tremendous amount of money invested in the fight against fraud and scam, The Association of Chartered Fraud Examiners (ACFE) notes that the modern financial industry is becoming increasingly susceptible to fraud due to ineffective controls and is unable to protect not only itself but also its customers (Enofe, Abilogun, & Omoolorum, et al., 2017). According to the same resource, the leading cause of fraud is weak internal controls and poor corporate governance and cultural practices. Furthermore, the risk of financial crime exists in absolutely every type of business. It is widespread both in developed and developing countries and varies significantly in its magnitude (Ozili, 2020). The ACFE estimates that the global cumulative annual damage from bank fraud is over the United States (US) $ 3.5 trillion and grows every year (Hussaini, Bakar, & Yusuf, et al., 2019).

Banking Fraud and Scam instantly swept over and absorbed many countries' banking sectors (The United States of America (USA), Russia, Europe, China) ten years ago and reached New Zealand in 2020 (Islam, 2020). According to Netsafe reports (2021), New Zealanders lost $23 million (16500 instances) million and $19 million (the most considerable single loss reported was approximately $840,000, and the average loss was $4,776.83 per case to online scam and banking fraud in 2019 and
2020 respectively. Actual numbers will be much higher, with many people not aware they are victims or too embarrassed to report it (Netsafe, 2021). Moreover, this trend is easy to trace through the mass media and comments on social networks. Additionally, «The Big Four» New Zealand banks (Australia and New Zealand (ANZ), Auckland Savings Bank (ASB), Bank of New Zealand (BNZ), and Westpac) suddenly posted about 40 fraud detection officer vacancies in January 2021 (LinkedIn website, 2021). Against the backdrop of the emergence of a new type of crime, the Reserve Bank of New Zealand published only one official bulletin, which described the possible types of financial crime and how to combat them many years ago (Dench, 1999). However, like science, crime does not stand still and is constantly evolving. In recent years, many new methods of fraud have emerged, such as scam grandparents or scam mortgage, which have not been described in detail by the federal bank and require special attention (Islam, 2020).

This research will build on existing research regarding card fraud and online transactions worldwide. The focus will also include the current realities of the financial and banking industry in New Zealand to understand different techniques that fraudsters use to mislead a potential victim and commit a crime. Moreover, in-depth research of the proposed approaches to prevent banking fraud and scams will be conducted. Furthermore, how the government and its agencies (Financial Intelligent Unit and Reserve Bank) can help mitigate financial crime risk will be investigated.

1.2 Background

1.2.1 Overview of the New Zealand Financial and Banking Industry

The financial industry (sector) is a wide range of profit companies that provide financial services to corporate and retail clients (Berger, Molyneux, & Wilson, et al., 2010). According to the Financial Stability Report (Official Reserve Bank of New Zealand, 2021), in all developed countries, the financial system consists of several layers: the function of control of financial activities is provided by the State (National Banks, Reserve Banks), while financial institutions conduct commercial activities and provide financial services to the society.

Figure 1 shows how the Reserve Bank of New Zealand regulates all financial institutions and manages New Zealand's financial market infrastructure to maintain a reliable and efficient economy in the country. New Zealand has a complex financial system with many strata and players involved. The Reserve Bank regulates the institutions depicted directly under the magnifying glass in this financial system chart (Reserve Bank of New Zealand, 2021).
Figure 1
Regulations area of Reserve Bank of New Zealand

FINANCIAL SYSTEM


Figure 1 also shows which institutions, markets, and infrastructures that make up the financial system and how they interact with each other. New Zealand citizens are performing financial activities in the middle of the entire financial ecosystem of the country's system. It outlines that the entire financial industry in New Zealand is under the control of The Reserve Bank of New Zealand, with the exception of global financial markets and investment opportunities.

Typically, the a country's financial institutions include all types of banks, investment companies, insurance companies, real estate firms, and New Zealand is no exception in this sense (Lin, 2013).

Figure 2 illustrates the breakdown of New Zealand financial institutions by total assets in June 2021.
Figure 2
Financial institutions’ total assets


Figure 2 shows that the banking sector dominates the New Zealand financial industry, with bank assets accounting for a considerable share of the total assets of the financial system (628 billion (BN) New Zealand Dollars (NZD) - 84%). Moreover, most of the financial industry (98%, except non-bank lending institutions) follows The Federal Reserve Bank of New Zealand rules and regulations.

According to Kensington (2021), private sector lending is the most important source of income. Figure 3 provides information about the structure of the personal loan portfolio of the New Zealand banking industry in 2021. It is worth noting that of the 27 registered banks in New Zealand, four large Australian banks (ANZ, ASB, BNZ, and Westpac) account for 85% of bank lending.
Figure 3
Sources of private sector borrowing

![Diagram showing sources of private sector borrowing]


Although 27 registered banks in New Zealand, four large Australian banks (ANZ, ASB, BNZ, and Westpac) account for 85% of bank lending (Figure 3). The five New Zealand-owned banks account for only 9% of the banking business. Direct capital market funding (issuance of corporate bonds) and non-bank lending institutions (NBLIs) together account for only 6 percent of non-financial private sector borrowing.

The dominance of foreign banks in the New Zealand financial industry can negatively and positively impact the country's economy, which is not the subject of this research.

1.2.2 Concept of Fraud and Scam

Over the past few years, the financial industry has made an enormous breakthrough in applying information technology to achieve business goals. It is now impossible to imagine that any financial institute could operate without modern electronic technology (Mason, & Bohm, 2017). The role of technology is to improve citizens' lives and simplify business transactions (Airehrou, Vasudevan & Madanian, et al, 2018). However, the development of information technologies in banking and their introduction into all aspects of financial life has led to the emergence of a new type of crime – banking fraud and scams (Hussaini, Bakar, & Yusuf, et al, 2019).
The word “fraud” has its legal meaning that varies from country to country (Kolapo, & Olaniyan, 2018). The first "fraud" was defined in 1888 by the US Supreme Court “when the defendant knowingly made a statement of material fact that is false and the complaint acts following that representation, reasonably believing it to be true”. However, Kautilya, in his famous document “Arthashastra” dated down around 300 before Christ (BC), detailed what we call “fraud” in the modern world of Chakrabarty (2013, July). For instance, Kautilya describes more than 30 ways to steal someone else's property: “what is realised earlier is entered later on; what is realised later is entered earlier; what ought to be realised is not realised; what is hard to realize is shown as realised; what is collected is shown as not collected.”

ACFE defined fraud as a "deliberate use of one's official position for personal illicit enrichment or misuse of company resources or to cause harm or use of an organisation's assets or resources" (Ozili, 2020). Alfian, Tarjo, & Haryadi (2017) described fraud as the use of potentially illegal means to acquire money or other property owned by a financial institution or individual by deception. The Federal Bureau of Investigation (FBI) defines fraud as “the illegal transformation or acquisition of resources or money under a pretence” (Hussaini, Bakar, & Yusuf, 2019). All of the above definitions of fraud boil down to the fact that fraud is a deliberate false provision of information to an individual or legal entity to deceive or mislead the victim, as a result of which the victim suffers material and moral damage.

In most cases, fraud can take the form of property theft, misappropriation of assets, and even manipulation of records and documents (blackmailing), but in most cases, fraud is supported by the concealment of theft (Enofe, Abilogun, & Omoolorum, et al., 2017). In other words, fraud is the conversion of stolen property or resources (Kolapo, & Olaniyan, 2018). Enofe, Abilogun, & Omoolorum et al. (2017) strongly believe that there must be three vital elements for fraud, Will, Opportunity, and Exit (escape way) which they call "WOE"; This abbreviation stands for the Will, Opportunity, and Exit (escape way), which this in turn refers to the triangle of fraud, which represents perceived pressure, perceived opportunity, and rationalisation.

However, the origin of the word "scam" is not precisely known, but the first mention dates back to the 1960s in the USA. Unknown sources of information suggested that the word originated in the jargon of carnivals, which were known to manipulate games to make them impossible to win (Upadhyay, 2018). The meaning of these games exactly fits the modern definition of committing fraud — “an illegal way of enriching or taking away finances, which includes deceiving or misleading third parties” (Gajjar, 2021). A scam occurs when a criminal fraudster tries to lure, threaten or scare a victim into giving up sensitive information or funds (Wyre, Lacey, & Allan, et al., 2020). However, scams
rely on deception, appear very genuine, and can be challenging to detect as they may seem like they are coming from a bank, business, or an individual. People who are caught out often face financial hardship or may be gullible or naive, especially with technology (Gajjar, 2021).

In the era of e-commerce and widespread bank cards and online payments, at the final stage of the scam process, fraudsters write-off money from a victim's bank card or account (Dench, 1999). According to the Reserve Bank of New Zealand, the difference between scams and fraud in banking is not significant, and one can be considered an integral part of the other (Dench, 1999). Moreover, the main goal of scammers is to gain access in various ways to the client's data or completely change the client's identity to seize assets or money (Gajjar, 2021). Because of information technology and communications development, modern fraudsters prefer to remain in the shadows, committing crimes via only online cold calling only (New Zealand Government, 2021). According to the same resource, the leading cause of fraud is weak internal controls and poor corporate governance and cultural practices.

1.2.3 Theoretical Framework of Fraud

In 1950, Donald Cressey launched the first formal research of banking fraud, arguing that there must be a good reason behind everything people do (Fitri, Syukur, & Justisa, et al., 2019). According to Joel (2018), a question such as "why do people commit fraud?" prompted Cressey to focus his research on what causes people to break trust. After interviewing 250 criminal fraudsters over five months, he concluded that people who commit fraud are usually capable of such acts due to the interaction between three factors: pressure (typically financial), perceived opportunities, and rational explanations for their actions (Said, Alam, Karim, & Johari, et al., 2018). For this reason, this theory has become known as the triangular theory (Figure 4) because it includes the three key aspects that motivate people to commit fraud.
Perceived pressure from some circumstance or event drives people to commit fraud (Bonsu, Dui, Muyun, Asare, & Amankwaa, et al., 2018). Joel (2018) described the primary forms of perceived trust as financial needs (possibly imaginary), job-related pressures and pressures as a way to get hold of something, and as a result of an inability to pay bills, drug addiction, or the pursuit of luxury.

Another critical corner of the triangle that leads to an increase in banking fraud is the opportunity. It is possible to significantly reduce fraud when possibilities are ruled out (Christian, Basri, & Arafah, 2019). The ability to commit financial fraud while remaining unpunished is critical in pushing people to commit fraud against financial institutions and their customers (Bonsu, Dui, Muyun, Asare, & Amankwaa, et al., 2018).

Rationalisation is the last corner of the triangle that Cressey discussed talked about in his research on banking fraud (Fitri, Syukur, & Justisa, et al., 2019). Said, Alam, Ramli, & Rafidi et al., (2017) defined rationalisation as a way to legitimize the concept or circumstances of a crime that is incompatible with people's self-beliefs, that is, to justify their actions. According to Joel (2018), this type of degenerative behaviour occurs to free oneself from guilt. Surprisingly, many researchers consider the fraud triangle an unfinished concept, challenging to apply in practice and suggesting different development paths. The authors of the diamond theory (Figure 5) claim that their approach is perfect for detecting and preventing banking fraud, as the theory spans four corners, adding the capability to the Cressey corners (Christian, Basri, & Arafah, 2019).
Moreover, in 2012 Crowe proposed a Pentagon-based theory (Figure 6) of banking fraud, adding two new elements to the triangle - capability and arrogance (Joel, 2018). The main argument for the imperfection of the triangle theory and its transformation into the Pentagon theory is that there have been significant changes in the environment and business practice (Joel, 2018). However, no specific explanations have been found from Pentagon theory supporters about the business changes in question. Besides, the authors of all theories of banking fraud were based on human qualities and vices that have existed for many hundreds of years (greed, the pursuit of luxury, impunity). Furthermore, based on three fundamental theories of banking fraud, the reasons for the committing of fraud in New Zealand remain implicit and unclear, which can be determined during research.
1.3 Research Aims, Questions, and Significance

As discussed earlier in this chapter, the financial industry plays one of the critical roles in the life of any country, making a massive contribution to Gross Domestic Product (GDP) and regulating financial flows within countries and beyond. According to the Reserve Bank of New Zealand (2021), the banking industry occupies more than 80% of the financial system of any country. It is not only the banking industry that suffers from fraud but also the financial system and the country as an entire organism. Various studies and surveys have indicated that banking fraud and scams are among the most critical problems in today's financial world (Ahmed, Madawaki, & Usman, et al., 2014).

After research the modern literature and articles on banking fraud and scams, a small amount of information was discovered about the current situation in New Zealand and the role of the Government and financial institutions in mitigating the risk of fraud. Moreover, the reviewed literature did not include a clear description of the most common types of banking fraud and scams in New Zealand or how New Zealand citizens can prevent or avoid fraudulent activities by using simple techniques and tricks.

The key aim of this research was to investigate banking fraud in New Zealand and create a simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud or scams. In addition, the research will help to understand technical aspects and types of bank fraud and scams in New Zealand. The research examined the New Zealand Government’s and financial
institutions' response in the prevention and control of bank fraud, including what has been done up until now and what else could be done in the future.

Based on the above, the objectives of this research can be formulated as:

1. To identify the forms of banking fraud and scams in New Zealand.
2. To examine the Government and financial institution's responses in the prevention and control of bank fraud in New Zealand, what has been done and what else could have been done.
3. To create a simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud and scams.

To achieve the research goals, the following questions were formulated:

1. What are the most common forms of banking fraud and scams in New Zealand?
2. What efforts should the Government (Reserve Bank of New Zealand, New Zealand Police) and financial institutions make to mitigate the risk of fraud for New Zealand citizens?
3. How can the New Zealand community protect itself from banking fraud and scams?

Once completed, this research is expected to bring value to the following stakeholders:

1. Fraud and Cybercrime Units within New Zealand banks to counter cybercriminal attacks and implement and improve anti-fraud approaches;
2. Reserve Bank and government agencies in New Zealand to analyse the situation around banking fraud and implement counteractions;
3. Bank customers to understand the situation of fraud in the financial sector and for further use in everyday life so as not to become a victim of fraudsters;
4. For students, corporate managers, various financial and non-financial institutions, academics who want to learn more about fraud, particularly ways to detect and mitigate the risk of fraud.

1.4 Research Process and Phases

The research process in this Thesis contains five acute phases. It is impossible to start the next phase without completing the previous stage and ending in a milestone. Figure 7 shows the high-level of research process progression and phases with the respective steps.
The first phase was intended to determine the research's objectives and pose questions to achieve the goals. According to Ioannidis (2018), the critical point of the first phase is to collect and read as much scientific literature and articles relevant to the research topic as possible. After intensely researching the world practices of the research topic, the researcher was well informed and became more confident in determining the purpose of the research. Moreover, in-depth research of the literature and world practices on the research topic helped to identify gaps and limitations in the existing literature, which made it possible to formulate the three research questions, the answers to which led to the achievement of the goals (Ioannidis, 2018). The research questions were formulated based on the researcher’s experience, literature review, current understanding of the research topic, and referring to the body of knowledge via informal interviews with industry professionals.

Furthermore, the formulated questions were subject to further scrutiny to ensure the use of correct banking terminology and design. In the last step of the Phase one, the researcher has discussed and decided the research objectives and questions with the supervisor and co-supervisor. Refer to Chapters 1 and 2 for an in-depth discussion and analysis regarding Phase one.
Phase two was commenced after completing the first milestone (Phase one and all the respective steps). In the Phase two, an mixed methodology was determined and preparation undertaken for the data collection process. In the Phase two, the most crucial steps to develop data collection tools (online questionnaires and face-to-face interviews). Existing research in the banking industry and discussions with the supervisor and co-supervisor have led to a mixed methodology (quantitative and qualitative). Descriptive statistics, clustering, and classification models were used when conducting the research using the quantitative methodology. For a qualitative methodology, an online questionnaire and face-to-face interview were used, which passed through two levels of expert assessment (supervisor and Otago Polytechnic Auckland International Campus Research and Ethics Committee) and tested on a sample group. Moreover, the Whakapapa Māori key principles were considered during the entire research. The author consulted with a Maori professional (Virginia Warriner) to ensure that the Maori research ethics are met. Whakapapa Māori principles allowed to follow the cultural, spiritual, and material values of Māori. This approach brought benefits to whanau, iwi, hapu, and the entire New Zealand community. Refer to Chapter 3 for an in-depth analysis of Phase two.

In Phase three, a pool of research participants were identified using the established and approved criteria approved by the Research and Ethics Committee of Otago Polytechnic Auckland International Campus. Moreover, a key milestone in the Phase three was to deploy ready-made tools (online questionnaire and face-to-face interview) from the Phase two and data collection. The target for the completion of the Phase three was to receive a minimum of 100 responses from banking services users through the online questionnaire and conduct five face-to-face interviews with banking industry employees. LinkedIn, the professional social platform was used to collect 100 responses from banking services users. Financial industry professionals were identified from the researcher's (currently an employee of a New Zealand bank) network and co-supervisor's (a former employee of a bank in New Zealand) network. Refer to Chapter 3 and the Research and Ethics application document for more detail in relation to Phase three.

In Phase four, the data was analysed. An essential step in analysing the data was to prepare the initial data and clean it up from missing values, various information noise, or incorrectly filled answers from the online questionnaire since raw data can lead to calculation and analysis errors and incorrect conclusions. Based on the final cleansed data descriptive statistics, classification, and clustering were carried out, with the aim of drawing the research's key conclusions. The milestone in Phase four was the formulation and testing of the hypotheses based on the findings from descriptive analysis. Phase four is described and discussed in-depth Chapters 4 and 5.
To complete the Phase five, the write-up was completed and the dissertation was submitted through the Moodle. The final milestone of the Phase five was to obtain a completed research manuscript, including research findings, discussions, conclusions, and recommendations for future research. Refer to Chapter 5 for in-depth detail regarding Phase five.

1.5 Chapter Summary

Fraud poses a threat to the continuing operations of an organisation and its interactions with external stakeholders such as customers, suppliers, financiers, and business partners, which can result in substantial financial damage (Kolapo, & Olaniyan, 2018). The banking sector plays a vital role in the financial system of any country and plays a vital role in the development of the national economy and the well-being of citizens (Enofe et al, 2017). However, if banks are to operate efficiently and make a significant contribution to the development of their country's economy, the industry must be safe, stable, and healthy.

Today, banking fraud is a significant threat to New Zealand's financial health and every individual in the country. Therefore, the key to the prosperity of the New Zealand economy and its citizens is the prompt identification, prevention, and of mitigating the risk of banking fraud.

In the process of combating fraud and scams, the financial institutions and government agencies (Reserve Bank of New Zealand, New Zealand Police), and the New Zealand community play a key role. Only practical cooperation of all three research participants in the process can significantly mitigate banking fraud or bring it to zero (Mason & Bohm, 2017). It makes sense to research banking fraud and scams in New Zealand and propose effective fraud and scam risk mitigation measures for all stakeholders. Additionally, researching the world's best anti-fraud and scam practices and comparing them with New Zealand's experience will close the gaps and improve the measures' effectiveness.
CHAPTER II: LITERATURE REVIEW

2.1 Introduction

Chapter 2 discusses the existing theoretical and empirical literature on banking fraud and scams around the financial world. Moreover, this chapter will review worldwide best practices used to mitigate the risk of banking fraud and scams that financial institutions and government agencies have undertaken.

In-depth research into banking fraud and scams was carried out and is described in the first and second sections; examining the reasons and causes for committing banking fraud. The literature review provides information on what factors drive people to commit fraud and assist in the development of measures to counter fraud before it is committed. An in-depth analysis of the types of banking fraud and scams will allow bank customers and financial institutions to recognise illegal actions the moment of suspicious activities arise and mitigate the risk of losses. Furthermore, a descriptive analysis of the most common scams in the world will help identify a fraudulent pattern in New Zealand.

The third section will focus on the role of financial institutions and government agencies in combating banking fraud and scams. An analysis of the experience and global best practices of financial institutions, Law enforcement, and Federal Banks will identify gaps in collaboration between all stakeholders in mitigating the risk of fraud and scams. Furthermore, it will offer effective measures to mitigate the risk of fraud for the financial industry and New Zealand citizens.

2.2 Banking Fraud and Scams

2.2.1 General Meaning of Banking Fraud

Fraud is a universal phenomenon that has existed since historical times and is one of the key enemies of the business world (Clementina, & Isu, 2016). Fraud exists in all walks of life, government, banking, export/import sectors, shipping, insurance, real estate, and more. Specialised organisations exist to combat it, such as Interpol (International Police) or the ACFE, which try to counter fraud internationally. However, it still exists and will continue to live in the future (Mbuguah, 2013).

Fraud in the banking sector is of the most significant nature, as it directly impacts the health and prosperity of the global economy and individual countries (Hakami, & Rahmat, 2019). According to Tawiah (2017), the magnitude of bank fraud cannot be known because much of it is undisclosed or undetected, and not all that is discovered is published.
The term "fraud" has many different meanings but is commonly used to describe the following adverse events (Tawiah, 2017):

a. Civil or criminal offence.

b. Misrepresenting the name of an individual or organisation.

c. Description of unfair transactions or contracts between individuals or companies that have caused damage to one of the parties.

d. According to Hakami, & Rahmat (2019), fraud is defined as “the deliberate act of one or a group of persons among management, employees or third parties, which results in financial loss and moral damage”. The above actions may include:

1. Manipulation, falsification of financial documents.

2. Misappropriation of assets by deception or misleading.

3. Suppression or omission of the consequences of a transaction from records or documents.

4. Accounting for transactions without content.

5. Incorrect application or non-application of accounting policies at all.

Ozili (2020) explains that among the many different definitions of fraud, the most common is that "fraud" is a general term that encompasses all technological and behavioural means by which one party tries to gain an advantage over another to obtain material and intangible benefits. Ozili (2020) explains that fraudsters use trickery, deception, surprise, and technology to get the desired result when committing fraud.

Chakrabarty (2013), defines banking fraud as an intentional illegal act or omission carried out in the course of a banking transaction or in order to perform it, aimed at obtaining an illegal profit, which brings financial damage to a bank and customers. Hakami & Rahmat (2019) proposes a similar but more recent definition of banking fraud, which is the deliberate act of an individual or group to change financial truth for selfish monetary gain using tricks (scams) and know-how (technological advances).

### 2.2.2 Causes of Banking Fraud

According to (Kaur, 2020), the causes of bank fraud and scams can be divided into two large groups: institutional and environmental/social factors. Moreover, Tawiah (2017) suggested dividing environmental/social factors into inadequacies and socio-economic lapses.
2.2.2.1 Institutional Factors

According to Tawiah (2017), the institutional factors for committing banking fraud are reasons that can be traced within the internal environment of the company. These reasons are the source of internal controls on the part of the company's management.

The leading institutional cause of fraud and scams is poor company process management and weak oversight (Almajir, & Usaini, 2020). Kaur (2020) suggests that, due to the inadequate oversight by the management of financial companies, the general perception of the environment is that the domain is safe to commit fraud. Ineffective company management will also manifest itself in inefficient processes, procedures, and policies, which will create an additional foothold for unauthorised gains (Almajir, & Usaini, 2020). In companies with effective oversight of compliance with policies and procedures, fraud can be committed by deliberately ignoring or violating procedures and policies (Bonsu et al., 2018).

Another reason for institutional fraud is the inexperience or carelessness of the company's employees, who can fall for the numerous tricks of the fraudsters (Tawiah, 2017). The chances are high that an inexperienced employee is unlikely to notice fraud and will be able to take the necessary measures to prevent it. For instance, the most common mistake new bank employees make is approving international bank transfers from scammed customers who believed they were making a genuine transaction.

A tired employee is a weak link in any company process. Overstretching is another reflection of poor management that can lead to fraud (Sharma, & Sharma, 2018).

Typically, the longer an employee works in one position and performs the same duties, the more proficient they become (Kaur, 2020). According to Tawiah (2017), an employee who does a particular job for an extended period may be encouraged by the thought that no one will uncover their fraudulent activities. This situation is also a prime example of poor management in a bank.

Low wages and poor working conditions also contribute to fraud (Bonsu et al., 2018). Low-wage employees who constantly deal with money are often tempted to embezzle employer or client money to meet their personal or social needs. Tawiah (2017) also agrees that greed, low wages, and poor working conditions drive people to commit crimes. These facts explain why internal fraud exists in the banking industry.

Employee frustration is another cause of fraud (Sharma, & Sharma, 2018). There is a high chance of fraud in a company where employees feel unobtrusive or unnecessary in terms of tangible and intangible bonuses or promotions. Such an employee may contribute to the committing fraud to
attract attention from the bank's management or to compensate for themselves in his way (Tawiah, 2017).

### 2.2.2.2 External/Environmental Factors

External and environmental factors can affect from outside of the company. Any financial company is part of and influenced by society (Kaur, 2020). If the banking industry is a part of the community and turns out to be morally or physically bankrupt, then the risk of fraud will be significant.

On the one hand, the banking industry is not immune to external and societal events (Almajir, & Usaini, 2020). According to Tawiah (2017), virtues such as honesty, decency, and good character are receding into the background in modern society. For society, the main goal is material wealth, and in order to achieve it, people are ready to disregard the law and moral foundations. Anyone who becomes rich immediately becomes famous and revered (Sharma & Sharma, 2018). It is a fact of contemporary society. The desire to become rich and famous is firmly entrenched in the social environment and is one of the reasons for committing banking fraud. However, the desire to become rich and powerful in one's social unit may be due to other reasons, such as cultural demands, cultivating life, or simply a desire to participate in an extreme event (Tawiah, 2017). Moreover, criminal motivation can be pathological, reflecting the offender's state of mind and encouraging fraud without the need for resources and wealth (Sharma & Sharma, 2018).

On the other hand, the material poverty of society can be the reason for committing banking fraud (Kaur, 2020). The desire to simply feed children or send them to study at school or university can transcend all moral principles and push people to commit illegal actions. Undoubtedly, this reason requires attention from any Government.

### 2.2.3 Types of Banking Fraud

Technological developments have transformed company visions and people's lifestyles. Modern technology has made life easier and more efficient. However, despite the many advantages of advanced technologies, numerous dangers come from fraudsters using online channels and bank cards to commit crimes (Kemp, 2020). In terms of the channel of committing, banking fraud can be divided into two large groups (Dvoryankin, 2021):
1. Internet banking fraud: sensitive information (bank card details, online banking credentials, identification (ID)) is stolen using the Internet.

2. Bank card fraud: the necessary information to commit fraud is stolen through physical contact with the victim.

2.2.3.1 Internet Banking Fraud

Currently, Internet banking fraud is becoming a more serious problem as the Internet continues to be an integral part of human existence and any cashless financial transaction in the world (Ushmani, 2019). Furthermore, despite the deep understanding of this issue and multi-million-dollar investments in security made by the financial industry and governments, users of financial services remain vulnerable (Shulzhenko & Romashkin, 2020).

One of the distinguishing characteristics and advantages of online fraud is that the perpetrator does not have direct contact (face-to-face meetings) with the victim, which significantly reduces the chances of being exposed (Kraiwanit & Srijam 2021). This method of fraud is gaining popularity every year, penetrating all spheres of public life. The lack of direct contact and the use of information technology makes it easier to obtain the personal data of potential victims. Just as many companies and services use personal information to set up targeted advertisements and offers to attract customers; fraudsters use this information to commit crimes (Kemp, 2020).

It is important to note that fraudsters mostly rely on modern technologies and unique capabilities and the classic psychological methods of influencing a victim, allowing them to mislead - scam (Kraiwanit, & Srijam 2021). Fraudsters most often use the gullibility of their victims when they disclose sensitive information, neglects or does not know the basic rules of Internet security.

2.2.3.1.1 Phishing and Smishing

One of the most popular and effective forms of fraud, in terms of achieving results, on the Internet are “phishing” and “smishing” (Shulzhenko, & Romashkin, 2020). The word “phishing” is a combination of two English words: "password and fishing." This method is often used to defraud victims using internet banking by posing as banks, tax authorities, medical institutions, and other social services (Dvoryankin, 2021). Smishing (Short Message Service (SMS) phishing) is the same thing, except it occurs via text messages. Scammers send a fake message to hundreds of randomly selected email addresses or predefined email addresses (targeted phishing), asking them to urgently log into the online banking system of a particular bank or enter the bank card credentials to confirm
the customer's identity or receive the payment (Shulzhenko, & Romashkin, 2020). The message contains a link to a fake website, where all the necessary information is collected to commit fraud (online-banking username and password, bank card credentials). With this information, fraudsters can do all sorts of things in the name of financial gain for themselves, such as ordering products online, transferring money from victims' accounts through their online banking access, and even taking out loans from other banks using the victim's data.

Fraudsters can construct high-quality responsive phishing sites that target banks and government agencies. Victims are led to these sites using various social engineering techniques in emails and SMS messages (Shulzhenko, & Romashkin, 2020). Moreover, Cloud technologies allow fraudsters to quickly stand up to phishing websites. Fraudsters often use domain names that look very similar to the genuine company’s name (Dvoryankin, 2021). Cheap domain name hosting services have made it easier for fraudsters to orchestrate phishing attacks. The increased use of mobile devices (and smaller screens) makes it more difficult for victims to detect a domain that looks genuine but is malicious.

According to the New Zealand Government (2021), banking services users receive phishing emails from fake Post Offices (parcel delivery), New Zealand transport agencies (car registration), and Inland Revenue Department (IRD) services (taxes refund).

Recently, this classic type of phishing attack has undergone many changes, mainly because more and more banks are sending one-time codes to confirm transactions via SMS (Ushmani, 2019). In this regard, scammers send emails to which they attach fake files, which allegedly contain statements with account history or requests for payment. Usually, attached files have extensions similar to the widely used ones but with minor changes. For example, instead of the "* .pdf" file, the "* .pif" file is used, and when such a file is opened, the virus is installed on the victim's computer (Dvoryankin, 2021).

Nowadays, the awareness of users about phishing attacks is increasing. Banks, government agencies, social media, and other web services warn their customers of various social engineering scams (Kraiwanit & Srijaem 2021). All this reduces the number of responses in the phishing scheme. For this reason, scammers need to be creative and develop new ways to scam (Dvoryankin, 2021).
2.2.3.1.2 Pharming

Pharming is a portmanteau of the two words "phishing" and "farming". This type of Internet fraud is similar to phishing, where a genuine website's traffic is manipulated, and sensitive information is stolen (Dvoryankin, 2021).

Through email or remote access, the fraudster distributes unique malware to users' computers, which, after launch, redirect calls to specified sites to fake sites that are almost indistinguishable from the original ones for the average user (Shulzhenko, & Romashkin, 2020). Once the victim settled on the fake site, the ultimate aim is to hand over sensitive information, such as account login credentials or credit card details. This information can then be used in crimes like account takeover fraud and identity theft. Figure 8 shows the pharming process.

Figure 8
Pharming scheme

This type of Internet fraud ensures secrecy of attacks, and user participation is minimised - it is enough to wait until the user decides to visit the sites of interest to the attacker. In most cases, scammers frequently use online banking, social services, shopping, or social media websites (Kemp, 2020).
2.2.3.1.3 Carding

Carding is another type of fraud in which a fraudulent transaction is made using a payment card or its details (card number, cardholder's name, expire date, and card validation code (CVV)), not initiated or confirmed by its holder (Dvoryankin, 2021).

Carding is usually committed in two ways. Firstly, payment card data is generally taken from hacked servers of online stores, payment and settlement systems, as well as from personal computers (either directly or through remote access programs, "Trojans," "bots" with the "form grabber" function (spyware used to intercept entered passwords and usernames)) (Shulzhenko, & Romashkin, 2020). One of the most enormous payment card fraud crimes was hacking the global credit card processing Worldpay and stealing more than the US $9 million using its data in 2009 (Dvoryankin, 2021).

Secondly, fraudsters try to guess or pick up customer payment bank card details using artificial intelligence and conduct many test transactions with various online stores via the Internet (Kraiwanit & Srijaem 2021). This guessing or selecting payment bank card data method is called a bank identification number (BIN) attack (Shulzhenko, & Romashkin, 2020). BIN is the first six digits bank card number that identifies a specific bank and the country in which it is located. This number is not a trade secret and can be tracked on BIN identification sites in the public domain. Fraudsters disguise their actions and therefore use popular and well-known merchants with a high transaction load. At the next stage of committing a crime, fraudsters try to identify the rest of the unknown bank card data by conducting thousands of test low-value transactions with various combinations of a 16-digit bank card number, expiration date, and CVV, this process is very time-consuming. However, if successful on the part of fraudsters, thousands of customers will incur losses without even being involved in the fraud scheme (Westpac, 2021). According to the same resource, scammers carry out BIN attacks at night, so this activity is difficult to recognise by merchants or customers. After conducting successful low-value or non-value transactions (loading bank card details into a website or payment merchant), fraudsters make large value transactions through online stores that interest them, such as buying computer hardware or jewelry.

2.2.3.2 Bank Card Fraud

The intensive development of modern information technologies in electronic payment systems relieves citizens of the need to have cash. However, along with the convenience of cashless payments, the risk of becoming a victim of fraud using payment bank cards increases. Currently, the number of transactions through automatic teller machines (ATMs) and payment terminals (with the physical use
of bank cards) is increasing exponentially (Samudra, & Qisthi, 2018). For this reason, the number of robberies and fraud-related bank cards (credit or debit) increases in the same proportion (Dvoryankin, 2021). When committing this type of fraud, the main goal of fraudsters is to steal information from bank cards or the bank cards themselves.

According to Samudra & Qisthi (2018), fraudsters can steal bank card data in four different ways:

a) Theft of the bank cards themselves from the owners in public places such as subways, hotels, or supermarkets;

b) The introduction of spyware parasites in payment terminals in supermarkets. When a customer pays with a bank card in a supermarket, the spyware reads and copies the data. This method is sporadic due to the complexity of installing spyware and the need to integrate payment terminals in supermarkets into the network.

c) Fraudsters bribe employees of shops or cafes. For example, the customer gives the credit card to the waiter, who, during the transaction, imperceptibly copies the bank card data.

d) By skimming. In this case, fraudsters copy credit card details or clone the entire credit card while the victim is making a transaction.

According to Embarak (2018), skimming appears the most popular and efficient way of stealing money from debit and credit cards.

### 2.2.3.2.1 Skimming

The word "skimming" comes from the English word "to skim" which means to read (Dvoryankin, 2021). This type of fraud with bank cards is reading information from their magnetic stripe using a unique technical device or skimmer. Moreover, scammers also try to find out the pin code of the victim's bank card by installing a miniature camera on an ATM or payment terminal (Aliet al., 2019). After receiving all the necessary information, fraudsters copy the bank card data to a blank, depersonalised bank card and withdraw money from an ATM (bank card cloning) or use the bank card data to make purchases over the Internet (Samudra, & Qisthi, 2018).

The magnetic stripe of the bank card stores information such as the plastic number, bank card expiration date, owner's name, service code (so that the ATM/terminal understands what functions the bank card has), and a verification code (similar to CVV) (Dvoryankin, 2021). The fraudster duplicates the plastic and gains access to the bank card account with this information. At the same time, they can
withdraw money anywhere in the world until the account holder contacts their bank to block the bank card (Ali et al., 2019). In the absence of two-factor authentication, fraudsters can also shop online.

To steal card data, skimmers use special devices that are attached directly to the ATM, as well as to any receiving slot of the bank card reader (Embarak, 2018). Fraudsters prefer to install portable magnetic stripe readers (skimmers) on ATMs or stand-alone payment terminals such as parking terminals. However, there are cases of installation of skimming equipment in hotels, cafes, and restaurants, in stores, which is risky for fraudsters, as it can lead to the discovery of a skimmer.

Figure 9
Skimming devices locations

Note. Figure 9 shows ATM vulnerabilities that fraudsters use to install skimming devices. Created by author.

To commit fraudulent transactions, fraudsters use the following equipment:

a) The magnetic stripe reader (Figure 10) consists of a small integrated circuit powered by batteries. Fraudsters place the reader in a plastic or metal case that mimics and fits onto an actual bank card reader of the target ATM or other device (Visa, 2021). This component allows attackers to obtain information encoded on the magnetic stripe of the bank card without blocking the actual transaction;
b) To read the victim's personal identification number (PIN) card, fraudsters install a miniature video camera at the ATM itself or nearby (Embarak, 2018). This camera is disguised as interior elements or advertising materials. Moreover, fraudsters can use a keyboard patch (Figure 11) to read the PIN. This keyboard looks exactly like the original one (Visa, 2021).
The greatest danger to the user is posed by foreign and street ATMs, especially those located in unlit areas - it is easier to install readers on them (Embarak, 2018). The safest are ATMs located...
directly in bank branches. The security service regularly checks such devices, bank employees and the collection service (Visa, 2021).

### 2.2.3.2.2 Shimming

To protect bank cards from copying or cloning, the bank began to issue Europay, Mastercard, Visa (EMV) cards equipped with a chip. The purpose of this chip is to store bank card data and protect it from unauthorized access (Kozodaeva, & Obydennova, 2019). According to Kasanda & Phiri (2018), data that is usually held on the bank card's magnetic stripe is copied to the cards with a chip. This chip contains additional security components that are not on the magnetic stripe. This fact means that fraudsters cannot duplicate the EMV chip, but they can use the data to clone a magnetic stripe or other types of fraud. However, chip bank cards can only be hacked under special conditions and require expensive hardware, which is a significant barrier to widespread chip bank card fraud (Ali et al., 2019).

Nevertheless, fraudsters have also adapted to the new conditions and began to use devices installed inside ATM bank card readers. This type of fraud is called "shimming" (Kozodaeva & Obydennova, 2019). The Shimm is a thin, flexible board (Figure 13) that performs the same function as a skimmer.

**Figure 13**

Shimming devices

Note. The figure illustrates shimming devices from Canada and Europe, respectively. [https://trends.rbc.ru/trends/industry/612d019d9a79470e54677745](https://trends.rbc.ru/trends/industry/612d019d9a79470e54677745) Copyright by Visa RBC.
An ATM bank card shimming attack is a man-in-the-middle attack in which a cyber-fraudster inserts a device into an ATM bank card reader, which intercepts and records data passing between the EMV chip and the ATM card reader (Kozodaeva, & Obydennova, 2019). This data can then be reused to clone the magnetic stripe bank card. EMV chip data and magnetic stripe data have different reference values (CVV), so the data received from the EMV chip bank card cannot be used to clone the magnetic stripe (Aliet al., 2019). Bank card shimming is not a chip bank card or ATM vulnerability (Kasanda, & Phiri, 2018). For this reason, there is no need to add protection mechanisms against this form of ATM attack. Counterfeit bank cards can be immediately detected if a proper authorisation procedure is followed during an ATM transaction (Embarak, 2018). This attack can only be successful if the issuer does not verify the CVV when authorising the transaction.

### 2.2.3.2.3 Trapping

The type of fraud with bank cards, when a fraudster steals the bank card itself from an ATM, is called “trapping” or another name for the “Lebanese loop” (Kozodaeva, & Obydennova, 2019). In this type of fraud, the fraudsters put a piece of photographic film into the ATM bank card reader (other material can also be used, more often plastic), cut in such a way that the bank card, falling into the bank card reader, does not return to the owner, but gets stuck and falls into a particular envelope (trap), which is subsequently extracted by a fraudster using special thin tools (Embarak, 2018).

There are two types of fraudulent activities that scammers use to trap. Firstly, when the bank card falls into the trap, the attacker finds himself “accidentally” next to the victim and invites him to re-enter the PIN code, motivating him with the fact that a similar situation happened to him the day before and this helped to return the bank card (Kozodaeva, & Obydennova, 2019). After "unsuccessful" PIN-code entries, the bank card is not returned to the user. The scammer advises contacting the bank for help and when the victim leaves, the envelope, and bank card are removed from the ATM by the fraudster (Saha, & Rahman, 2018). As a result, the fraudster has the victim's bank card and information about their PIN code. Secondly, the fraudster is next to the ATM and waits for the victim to leave. In this case, the fraudster does not receive information about the bank card PIN because they do not interact directly with the victim (Saha, & Rahman, 2018). The second method does not allow using the bank card to withdraw cash from an ATM due to the lack of a PIN, so fraudsters use a stolen bank card to make purchases over the Internet.

However, the purpose of trapping can be not only a bank card but also cash. This type of fraud is also committed using an ATM and a bank card called cash-trapping (Hasham, et al., 2019). In this
In the era of modern technologies, new opportunities open up for humanity to invest capital, pay for goods and services, and find their other half (Gajjar, 2021). For this reason, the use of bank cards, and online payments are becoming more and more popular among all segments of the population worldwide. The emergence of new opportunities provides benefits for a comfortable life and increases the chances of being scammed and losing money (Wyre et al., 2020). Every new opportunity to improve life through the Internet leads to the emergence of a new type of scam. For instance, the opportunity to invest in Crypto or shares has led to investment scams, or the chance to find a loved one led to romance scams (Gajjar, 2021).

Regardless of what is being deceived (love, investment, goods), scammers (the person who is committing a scam) try to intimidate, lure, or instill hope into the victim (Wyre et al., 2020). However, all types of scams are based on deception and misleading. It looks heartfelt and can be challenging to detect, as it may appear to come from a legitimate company or individual (relatives or friends). When the victim ultimately trusts the scammer and gives out confidential information (banking or ID credentials), the scammer steals money from the victim's accounts. Trapped people often face financial hardship and can be gullible or naive, especially with technology or relationships with others (Gajjar, 2021).

Scammers are experts at manipulating people's trust and imitating genuine people or companies (Hamidah, 2018). They have sophisticated stories that play on emotions such as fear, loneliness, desire, and compassion to trick people into making decisions regarding the money they would not otherwise make. Scammers take advantage of people by preying on vulnerabilities such as isolation, age, financial hardship, language barriers, and minimal computer skills (Upadhyay, 2018). A scam happens when someone has been tricked into willingly authorised a transaction.
There are several opinions about what fraud and scams are in modern literature and the differences between these concepts. According to the Reserve Bank of New Zealand (2021), the difference between scams and fraud in the banking sector is insignificant. That is, a scam is one of the stages of fraud. In this context, fraud results from a successful scam (Dench, 1999). Murugesan & Chidambaram (2021) agree that scam and fraud are not fundamentally different since both of these actions pursue the same goal - theft of funds. Kaur (2020) believes that a scam is a type of banking fraud along with internal fraud, phishing, and even money laundering. However, all say that both concepts are negative and aimed at stealing money from people or companies. Moreover, according to New Zealand Financial Markets Authority (FMA) (2021), other names for scams include a con, fraud, rip-off, racket, hustle, sting, but it is a form of theft.

According to the annual New Zealand Netsafe Report (2021), in world practice, the most common types of scams, in terms of the number of events and financial losses, are an investment, romance, and phone call scams (29%, 19%, 21% of all losses respectively).

### 2.2.4.1 Investment Scam

Investment is the financial activity of companies or individuals in which funds are invested in a specific project, company, or service to generate positive returns and maintain or increase the value of assets (Lacey et al., 2020). The prosperity of modern technology opens up new investment opportunities for both companies and individuals. The development of new ways of investing accumulated funds has led to a new type of fraud - an investment scam (Salsabila, 2018).

Investment scams or "get-rich-quick" scams are specific to financial products and services such as stocks, bonds, managed funds, foreign exchange, digital currency, and investing or trading through an online or computer-based trading platform (FMA, 2021).

Fraudsters can work alone or in groups. They can target specific groups like clubs and churches, and individuals, but most of common target of investment fraud in older people because many are not computer savvy and are naive (Chariri et al., 2018).

In world practice, there are several types of investment scams:

1. Ponzi Schemes: When a fraudster claims to be offering a legitimate investment. In this type of investment scam, scammers build a pyramid scheme. Scammers take money from one victim, keep it for themselves, and then use the funds of other victims to return it the money to the first victim (Hamidah, 2018).
2. Affinity Fraud: Victims are trusted by people, such as religious, social, or cultural groups (Padil et al., 2020). They abuse the trust existing in these groups to steal money.

3. Boiler House Fraud: Involve teams of scammers who call strangers for non-existent, useless, or overpriced investments and then claim that the investment has failed (Lacey et al., 2020). At the same time, scammers do not hide from their victims and continue their activities.

4. Stock, Securities, and Digital Currency Fraud: Where fraudsters do not intend to buy from the client, citing extensive investment experience (Padil et al., 2020). Moreover, scammers can use a non-existent or legitimate company for investment and provide the client with their investment account to transfer money.

According to FMA (2021), the most common types of investment scams are online-share trading and digital currency (Non-fungible Tokens (NFT) tokens or Crypto). Fraudsters will pose as legitimate investment brokers and advise victims that they can get them some unbelievable returns on their investment, all for a low investment of a couple of hundred dollars (Lacey et al., 2020). Victims will then be shown some visually persuasive graphics while the fraudsters will continue a dialogue for them for what may be weeks, months, or even years, all the while telling them how well the investment is performing (Salsabila, 2018). When the victim wants to withdraw the funds, the fraudsters will advise that a withdrawal fee must be paid to do this, thus siphoning more money from the victim. These fees will steadily increase, and the victim will never see any actual monetary returns, while the fraudsters essentially can do what they like with the money. Victims will then try to recover their funds any way they can and usually defer to fake "scam recovery services," often managed by the same fraudsters purporting the original investment scam (FMA, 2021).

The problem of investment scams can be avoided or mitigated if victims understood the indicators of investment scams:

1. A potential victim receives an email or a phone call (not the client who found a place for investment, but the investment company found a client). Scammers are known to trade information on potential targets, including people who have previously invested in fraud or legitimate investments or have shown interest in investing, for example, by completing an online survey (FMA, 2021).

2. Scammers offer high profits with little or no risk of loss. In finance and investment, higher returns almost always mean a higher risk of losing some or all of your money (Hamidah, 2018).

3. The offer is valid for a “select few” or “for a limited time” (Salsabila, 2018). Such statements are often a gimmick to make the victim feel special and encourage them to invest.
4. The investment company or broker is not on the Financial Service Provider Register (FSPR) or is based abroad and does not have a physical address in the client's country. Fraudsters prefer to be based in countries with little control over fraudsters (Padil et al., 2020).

2.2.4.2 Romance Scam

Romance scams via the Internet originated around 2007 or 2008 with roots in paper mail fraud (Sorell, & Whitty, 2019). However, with the advancement of technology and the ubiquity of the Internet, paper mail fraud has become meaningless. Fraudsters’ romance scams are carried out through many different communication channels (Shaari et al., 2019). Figure 14 shows that romance scams are often carried out through online dating sites, but scammers can also use social media or email to establish contact. Furthermore, the most popular channel to commit a romance scam is the Internet - 88.5% of all events (social networking, mobile applications, Internet, email) (Australian Competition and Consumer Commission (ACCC), 2021). However, there are cases when scammers call their victims as first acquaintances. A romance scam is sometimes referred to by other names such as catfishing, the online dating romance scam, or the sweetheart's scam (Sorell, & Whitty, 2019).

Figure 14
Communication channels for romance scams

A romance scam is a way to mislead a potential victim, which involves encouraging a romantic relationship with the victim, gaining deep affection or sympathy, and then using the victim's feelings to commit fraud (Whitty, 2018). According to Barnor et al. (2020), the romance scam aims to access the victim's money through bank accounts, bank cards, or national identification numbers, or they can coerce a victim involved in a scam to commit fraud on their behalf.

As a rule, to commit fraud, scammers create fake online profiles through social networks or online dating websites to lure the victim (Netsafe, 2021). Fraudsters prefer to use fictitious names or specifically use the names of real people who are trusted in the community, such as military personnel or relief workers working overseas (ACCC, 2021).

The main distinguishing feature of romance scammers is that they demonstrate solid emotions and deep affection in a short period and offer the victim to move the relationship from the dating website to a more closed channel (email, phone, or messages) (Te Ara Ahunga Ora, 2021). Scammers are ready to do anything to gain the victim’s trust as quickly as possible. They prefer to use loving and affectionate words, love poems and songs, share "personal information", send low-cost gifts (Sorell, & Whitty, 2019). When gaining trust, the scammers take their time and are very patient, sometimes they are ready to wait months to win the victim ultimately (Netsafe, 2021).

After the fraudsters gain the victim's trust and the victim's emotional defences weaken, amid romantic feelings, the fraudsters will ask the victim (hinting or directly) to transfer money and/or send gifts under various pretexts (Shaari et al., 2019). In addition, the scammers offer to maintain a general budget and lure the victim's bank card or online banking data.

Money lost as a result of romance or online dating scams is almost impossible to retrieve; banks refuse to reimburse funds lost as a result of romance scams since, according to the rules of international payment systems (Visa, MasterCard), such transactions are always authorised by the holder of a bank account or bank card and are performed using the high-security level (PIN, CVV, online-banking credentials) (Netsafe, 2021). However, for many victims, the loss of deep affection and disappointment in a loved one is more complicated than financial loss, there have been cases where a break in a relationship due to a romance scam led to the victim’s death through suicide (Whitty, 2018).
2.2.4.3 Phone Scam

The development of the telephone industry, smartphones, and cellular networks makes the life of humankind more convenient and efficient. However, the development of cellular telephony has provided fraudsters with another way to steal money from people - a cold-call scam (Tu, et al., 2019).

Fraudsters are becoming more sophisticated and persuasive in their approaches to misleading potential victims into believing they are trustworthy and that an immediate solution or payment is required to resolve a problem (New Zealand Police, 2021).

Cold calling to anyone in the world is relatively inexpensive thanks to Voice over Internet Protocol (VoIP) calls, which provide voice communications over the Internet. The customer thinks the call is from a regular phone (Bidgoli, & Grossklags, 2017). According to the same resource, localised phone numbers can appear as if the caller is in the country where the potential victim is, giving immediate credibility. Moreover, scammers use phone number spoofing technologies (impersonating another person or company) - number spoofing (Netsafe, 2021). When using this technology, the victim will see on his smartphone screen that the call is being made from a bank, government, or other legitimate company. However, as with all different types of fraud and scams, fraudsters' goal is to gain access to the victim's data (bank card or online banking credentials) (New Zealand Police, 2021).

To find out the phone number of a potential victim, scammers can use a great variety of tricks, such as:

1. Fraudsters buy databases with phone numbers via the Internet (mainly the Darknet) (Tu, et al., 2019).

2. Customer number data is sometimes sold by unscrupulous employees of companies, including banks, telephone companies, or social networks (Bidgoli, & Grossklags, 2017). Such databases can contain phone numbers and other personal information of users - age, gender, debit and credit transactions, physical address, ID.

3. Victims often indicate their phone numbers in social networks, forums, and even online stores (New Zealand Police, 2021); scammers hack a poorly secured account and get a phone number. Sometimes phone numbers are publicly available on social media, and scammers simply collect them.

4. One of the most unusual and rare ways to get a potential victim's phone number is to ask someone on the street for a phone number to make an urgent call (Bidgoli, & Grossklags, 2017). This method allows fraudsters to evaluate the victim and choose the most acceptable one. Usually, scammers are presented as decent-looking young people who are more likely to be given a mobile
Phone for them to call the accomplices who will have the number of the future victim (Tu, et al., 2019).

5. Fraudsters collect data manually from various property sales sites or job search sites where potential victims post personal information (Netsafe, 2021).

6. The most expensive and technologically complex way to collect phone numbers is by parsing (New Zealand Police, 2021); scammers use artificial intelligence to brute force and randomise numbers. Scammers are trying to guess the phone number.

There are many different tricks that scammers use to mislead victims. According to the New Zealand Police (2021), the most common calls are from a bank or other financial institution, technical support or personal computer (PC) repair company, and government agencies (IRD, immigration, post office, hospitals, police) and when using any tricks to mislead the victim, the scammers are aware of legal companies' services and products.

In the event of a call from a bank or other financial institution, the scammers try to convince the victim that there is a problem with their bank account or credit card (Westpac, 2021). For example, they say that the bank has detected suspicious transactions or activity (someone is trying to sign on from another country) and, that it is necessary to verify the activity and prevent fraud (Murugesan, & Chidambraram, 2021). Scammers say it is necessary to identify the client and offer to do it in two ways. The contract number identifies the first method that the client concluded at the bank branch when opening an account (Westpac, 2021). Naturally, not a single client knows this number, and then the scammers offer to identify the client through bank card details or online banking.

In the case of a call from technical support, the scammers introduce themselves as employees of internet service providers or software companies. According to Netsafe (2021), there are three most popular scenarios for misleading a victim, but they all lead to the same outcome - installing remote control software on the victim's device. The scammers say that the client has problems with the Internet or internet speed or that hackers are trying to access the victim's device. To fix the problem and ensure security, scammers ask the victim to install remote control software, after which they gain control over the device, where they find all the data they need to steal money (New Zealand Police, 2021).

A call from government agencies is not very different from a call from a bank. For example, scammers say the victim needs to pay additional fees or expects a refund of overpaid fees (Netsafe, 2021). To identify the client and make a payment or refund, fraudsters ask for bank card details or online banking credentials, after which they perform fraudulent transactions.
Emergency phone call scam is usually targeted at older people who have grandchildren. In this case, the scammers use the feelings of love and deep affection of grandparents to take money away. This type of scam is called the grandparent phone scam (Netsafe, 2021). Typically, the scam starts with scammers pretending to be grandchildren, lawyers, hospital workers, or police, they call older people and explain that their grandchild is in a difficult situation, which requires money to resolve (Salvin, & Lepcha, 2019). Loving and naive grandparents are nearly always ready to help and transfer money to the scammers' bank accounts to help their grandchildren.

2.2.4.4 Other Scams

There are a considerable number of different types of scams in world practice. All of them are types of fraud with bank cards and online banking but compared to the investment, romance and cold call scams do not bring large profits to fraudsters (Gajjar, 2021).

Identity theft occurs when someone steals a person's personal information, including name, bank account number, credit card information, and social security number, often through mining (Golladay, & Holtfreter, 2017). In this case, the goal of the fraudsters is to use personal information to verify ID and access a bank account, open and use credit cards, take out loans, use health insurance to pay bills, or file tax returns for refunds (Wyre, et al., 2020).

Inheritance, lottery, donation, or event ticket fraud is committed through any possible means of communication (phone, mail, and Internet). A potential victim is sent information about receiving a prize or entering a legal inheritance and it is necessary to transfer a certain amount of money in favor of a lottery organiser, fundraiser, or lawyer to complete all documents (New Zealand Government, 2021).

Subscription scams offer low-cost or complimentary products and services, mainly by posting social media advertisements (Badawi et al., 2019). Usually, scammers offer to sell cheap weight loss products, healthy food, medicine, home appliances, and electronics. One notable recent example is the distribution of fake brand advertisements via Facebook, such as Dyson and Samsung, which offered to sell at $3 per item (Westpac, 2021). After the victim pays for the product, he automatically enters into a regular (daily, monthly) subscription to other non-existent services (Badawi et al., 2019). Surprisingly, from the point of view of the law, this type of scam is legal, since when making a payment for a product, the client is invited to familiarise himself with the term and conditions, where all payments and subscription details are spelled out (Netsafe, 2021). Unfortunately, the client does not read this document and makes a payment, agreeing with everything written.. This subscription is
much more expensive than any goods or services provided. Moreover, this subscription will be automatically extended, and there is no way to cancel it except to ask the issuer of the bank card to cancel and replace the bank card (Westpac, 2021).

Employment scams involve fraudsters advertising false jobs on recruitment websites or the Internet in the hope of luring a victim into applying. The fraudster "employs" the applicant and tells them either that as part of their job, they need to receive "payments" to the business into their account, and also "pay" suppliers to the company from their account (Shree et al., 2021). The fraudster "pays" the applicant for doing this. Another way fraudsters use these scams is to get the applicant to send a copy of their driver's license, bank account, and other personal information to take over their identity to steal their money (Vidros et al., 2017).

Since March 2020, the global COVID-19 pandemic has caused many problems worldwide. Unfortunately, scammers have not stood aside and used the pandemic to enrich themselves and deceive people worldwide (Murugesan, & Chidambaram, 2021). Against the background of news about the spread of the COVID-19 virus, panic among citizens of many countries, a shortage of goods in stores, and the departure of many companies to online channels, attackers have intensified in terms of the spread of malicious software, phishing emails and phone scams aimed at obtaining personal information of citizens and stealing payments (Lallie, et al., 2020). Besides, according to Unite against COVID-19 website (2021), COVID-19 has provided scammers with the chance to take advantage of people’s vulnerability and fear. The same source described new types of scams worldwide: online shopping – scammers have created fake online stores to sell goods that do not exist; income replacement - scammers are presenting job and employment offers to work from home or set up and invest in a 'business opportunity'; dating and romance are nothing new, but due to lockdown and isolation it opened new horizons for fraudsters.

2.3 The Government’s Agencies and Financial Institutions Roles

The role of government agencies and financial institutes in mitigating and combating banking fraud and scams cannot be overemphasised. For instance, positive results in combating financial crime in African countries were achieved with entire interaction and understanding between citizens, financial institutions, supervisory and regulatory authorities (Reserve Bank), and law enforcement agencies (Ahmed et al., 2014). According to Ahmed et al. (2014), government structures play a crucial role in ensuring the sustainability and efficiency of the banking sector to build trust and stability in the system. Clementina & Isu (2016) invites banks and governments to work together domestically
and at the macro level to attract reputable foreign experts in fraud prevention and detection and security management to save the country from the hardships of increasing cases of banking fraud and insecurity. Another important aspect of fraud prevention is exchanging information and openness between industries, citizens, and government agencies. In this regard, the primary tool that allows citizens to avoid fraud and organisations to prevent is the availability of accurate, up-to-date online information (Baz et al., 2017).

2.3.1 Financial Institutions Roles

Due to the seriousness of banking fraud and scams, customer protection has become one of the most critical prerogatives for all financial institutions (Tawiah, 2017). Moreover, at the time of fraudulent transactions, only banks stand between fraudsters and customers and can stop the crime (Joel, 2018). For this reason, the management of all financial institutions should understand the seriousness of the fraud and scam problem and take adequate measures to protect their customers and companies. Implementing anti-fraud strategies is becoming popular in modern banking. However, an anti-fraud strategy may be different for each bank, and depend on the size of the bank, the total amount of funds invested, and the overall environment at the national and international level (Doeland, 2017). Despite the implementation of anti-fraud strategies, the total damage from and the number of fraud and scam events is still rapidly growing both in every country globally (Tawiah, 2017). Thus, the effectiveness of the anti-fraud measures taken is questioned. Hussaini et al. (2019) believe that general anti-fraud and scam procedures for all financial institutions should include an anti-fraud strategy based on fraud identification and detection, and fraud prevention, identification, detection, and prevention are parts of one system and cannot exist without each other.

2.3.1.1 Fraud Identification and Detection

Various strategies for identifying and detecting fraud are plans implemented to efficiently and quickly detect fraud cases that bypass preventive measures so that the financial institution can take appropriate corrective action and avoid financial and customer losses (Enofe et al., 2017).

Bank employees are one of the main links in all banking processes. For this reason, every financial institution and every employee should know and be able to identify all types of fraud and scam at the time of it being committed, common in the world community, the reasons and methods of committing fraud, as well as the prospects for the emergence of new types of fraud (Hussaini et al., 2019). To be successful in understanding the main global trends in banking fraud by the bank's
employees, employers need to conduct regular (monthly) training for all employees, from specialists to senior management (Hasham et al., 2019). As practice shows, the most effective fraud and scam identification training is training based on successful and unsuccessful examples from world practice. Furthermore, incorporating a risk culture into all bank processes would avoid internal fraud and increase employee awareness of all the risks that may arise in their day-to-day work (Hussaini et al., 2019).

However, along with educated employees, the bank’s use of modern information technologies and their integration into all processes allows them to achieve high results in detecting fraud (Alfian, et al., 2017). Traditional transaction tracking systems check customer transactions against a predetermined set of strict rules (Joel, 2018). According to the same resource, if a deviation from the rules is detected, the transaction is automatically identified as suspicious, after which the fraud analyst must manually check the transaction. For example, a customer physically used their bank card in New Zealand, and in five hours they used the same bank card in India. That is impossible and might be easy to pick as a fraud for the banks or when a senior customer made a transaction with a dating or gambling merchant for the first time. However, applying the same rules uniformly to all situations increases the risk of false-positive transactions alerts that require review (Joel, 2018). In such cases, the everyday transactions of customers, for example, using a bank card abroad, the emergence of new hobbies, or simply a change of preference, would be considered fraudulent, which would lead to the blocking of the transaction and, as a result, the loss of customer loyalty.

The introduction of artificial intelligence technologies, including machine learning and Big Data methods, prevents blocking genuine activities and mistakes by bank analysts (Gyamfi, & Abdulai, 2018). For example, a team of employees at one of the largest Dutch banks Algemene Bank Nederland and the Amsterdam and Rotterdam Bank ABN AMRO) has developed a tool based on Unsupervised Machine Learning. This tool detects anomalies, or so-called outliers; operations that differ from the usual scenario with an 85% success rate (Gyamfi, & Abdulai, 2018). The use of artificial intelligence reduces false positive alerts and helps to prevent fraud and scams successfully.

The use of internal control mechanisms at individual departments in the bank helps reduce operational risks and detect potential fraud and scams (Kolapo, & Olaniyan, 2018). According to Tawiah (2017), invoice reconciliation, electronic surveillance, senior management scrutiny, cash checks, fraud audits, internal controls reviews, and an internal anti-fraud hotlines are the most effective ways to detect fraud and scams in companies.

Bank customers make a massive contribution to the detection of banking fraud and scams. Bank call centres receive thousands of calls from customers related to unauthorised transactions on
their accounts (Hussaini et al., 2019). Unfortunately, many banks follow a definite pattern (cancel/replace a bank card, lodge a dispute) and do not think about analysing and using the information received from customers (Hussaini et al., 2019). One positive example of acting on fraud information from customers was the opening a fraud call centre by some banks (Westpac, 2021). These fraud call centers are staffed by highly qualified operators who interact with customers and a team of fraud analysts who analyse transactions and identify fraudulent patterns.

### 2.3.1.2 Fraud and Scam Prevention

Fraud and scam prevention means preventing fraud before customers or the bank itself incurs losses. In other words, fraud and scam prevention includes efforts to reduce the incidence of fraud and scam to zero (Gyamfi, & Abdulai, 2018). Typically, it is much cheaper to implement fraud and scam prevention measures than to detect fraud and scam and compensate for damages in the event of fraud and scam (Tawiah, 2017).

Fraud and scam prevention is based on the bank's continuous improvement of key business processes. The first step is to identify weaknesses in the existing systems and processes of the financial institution and enforce controls (Hussaini et al., 2019). The introduction of these measures will reduce the opportunities for fraud and scam and warn potential fraudsters that the company is actively monitoring its business (Tawiah, 2017).

In the global practice of combating banking fraud and scams, there are various fraud and scam prevention methods based on interference with the company's technical, political, and human model (Mason, & Bohm, 2017). Using proactive strategies prevents banking fraud and scams and preserves the integrity, security, and authenticity of financial transactions.

Human interventions, which may include unexpected performance audits, employee training, and development programmes, verification of references from previous employment and credit history of potential employees, verification of customers and their partners, setting transaction and credit limits are among the preventive measures to prevent fraud and scam (Hussaini et al., 2019). Moreover, company employees need to have clear roles and a transparent escalation system/process if a problem cannot be resolved (Alfian et al., 2017). A risk-based corporate culture and educating employees about ethical standards reduces the risk of fraud and scams in the workplace. In addition, some companies have shown that a fraud and scam prevention mechanisms should include segregation of duties (authorisation, recording, verification, and processing), limits, authorisation and approval procedures, and control over access to resources and records (Enofe et al., 2017). The most advanced banks
combating fraud have their own fraud investigation units (Alfian et al., 2017). The fraud investigation team's mission is to investigate the incidents of fraud and scam and advise other departments of the bank and the Police to prevent similar incidents in the future (Alfian et al., 2017).

Fraud prevention currently includes technological methods used to prevent fraud and scams, including periodic updates of the technologies used, transaction limits, information access control, an anti-fraud hotline, a security mechanism, anti-virus protection, and password protection (Hussaini et al., 2019). Tawiah (2017) believes that fraud and scam prevention requires adopting an appropriate anti-fraud mechanism that is implemented within the business unit, such as access control, implementation and enforcement of a security mechanism, and physical security control systems. The establishment of an internal audit or fraud review department can ensure that the technology used is periodically updated and that performance is strictly monitored (Gyamfi, & Abdulai, 2018).

In addition, reviewing with company policies, improving or developing policies such as reporting policies and procedures used and communicating them to employees, communication and ethics policies, anti-fraud policies, reviews of the strengths and weaknesses of fraud and scam, strengthening the role of the audit committee, and imposing penalties and disciplinary action, are examples of effective fraud prevention mechanisms (Cross, & Blackshaw, 2015). Thus, introducing fraud prevention measures can increase loyalty from existing customers and attract new ones.

One of the most effective fraud and scam prevention measures is a collaboration between different financial institutions and payment services (Doeland, 2017). Any single bank is a closed system (Baz et al., 2017). Fraud in an isolated system can only be detected in one system and not in the entire banking industry (Doeland, 2017). Subsequently, the fraud will spread like a virus and affect the whole system. However, with an advanced system of data exchange between financial institutions, the fraud will not spread to the entire system. Even though this method is very delicate due to different privacy acts and laws, some European banks have agreed that banks will no longer compete in security and combating fraud, which led to the exchange of information between banks, cooperation, and trust (Doeland, 2017). In this context, we are not talking about the interaction of client databases or any sensitive information. However, sharing experiences about past cases of fraud or new ways to identify and prevent fraud will increase the chances of the entire banking system to significantly reduce the level of banking fraud and scams (Baz et al., 2017).
2.3.2 Federal Banks

The Federal Bank of any country plays a vital role in managing the national economy. The role of federal banks is to regulate and monitor the financial system and ensure its development, prevent financial problems that could undermine the credibility of the system, and promote sustainable growth (Tawiah, 2017). The ubiquitous role of the Federal Bank is assessed in the light of its constant monitoring of the domestic and international economy. Knowledge and understanding of the economic environment are the primary information source for economic planning (Alfian et al., 2017). Furthermore, effective policies and the involvement of the Federal Bank in the process of reducing the risk of fraud and scam can increase public confidence in the financial sector and reduce the number of cases of fraud and scam (Hasham et al., 2019).

Federal banks act as a supervisory and regulatory body of banking systems. One of the main interests of federal banks is to ensure that commercial banks establish comprehensive and effective internal controls. (Hasham et al., 2019). These measures will minimise the incidence of fraud, and whenever fraud occurs - detect and prevent further attempts. The internal control system should have the following attributes: dual oversight, segregation and rotation of duties, effective and independent oversight functions, clearly defined levels of authority and responsibility, and an influential audit committee (Ahmed et al., 2014).

Federal banks ensure that commercial banks comply with rules and regulations through exhaustive scrutiny of internal audit reports (Ahmed et al., 2014). Federal banks ensure that the board and management of the bank take appropriate steps to remedy the deficiencies raised in the audit reports (Tawiah, 2017). Supervisors should also work with external bank auditors to ensure that bank’s internal audit program is comprehensive, adequate, and efficiently implemented (Hasham et al., 2019). The supervisory authorities should also conduct a thorough investigation of the bank's activities. To enhance the ability of supervisors to carry out their duties effectively, they must be appropriately trained and equipped with modern technology (Tawiah, 2017).

Although the primary function of all federal banks is to regulate monetary policy, in the fight against fraud, they play a crucial role in creating and establishing information exchange between all stakeholders in the process (government authorities, financial institutions, media, the international community, the population of the country). (Hasham et al., 2019). Sharing information between all stakeholders can be a crucial component in fraud and scams prevention. The exchange of information helps to track all trends and innovations in fraud and scams and develop solutions to combat the spread of fraud at the country level (Doeland, 2017).
Another point on the information-sharing strategy of federal banks is creating and maintaining of the “Know Your Customer” (KYC) system. This system will allow all stakeholders in the financial industry to check the decency of all involved in financial transactions before or at the time of their commission and to prevent fraud and scams in time (Baz et al., 2017). One of the interesting modern projects in information-sharing is the interaction of federal banks with global search engines on the Internet (Google). The project aims to mark legitimate company websites and block company websites that posted fraudulent advertisements (Doeland, 2017).

Raising the financial literacy of all stakeholders and building trust in financial institutions is critical for federal banks to prevent fraudulent activities in the financial market (Engels et al., 2020). One of the most important actions in this area is to create a coverage system of anti-fraud and scam activities in the media and via the Internet (Grohmann et al., 2018). This will help increase literacy and recognition of fraud and scam types, reduce the tolerance for violations, and strengthen bona fide market participants (DeLiema et al., 2020). For example, the Central Bank of Russia (2021) is recruiting the most popular television channels to participate in a financial literacy campaign featuring financial industry professional experts and citizens affected by fraud and scams.

Federal bank awareness campaigns aim to spread awareness of financial fraud and scams and underlying malpractice, including potential risks and remedies (Engels et al., 2020). Furthermore, information campaigns in federal banks should help build an understanding of the responsibility and inevitability of punishment for fraud and scams among banking services users and banking employees (DeLiema et al., 2020). For instance, as part of the Saudi Arabian National Bank outreach campaign, they conducted field visits to financial institutions to build zero tolerance for illegal actions among employees (Baz et al., 2017).

2.3.3 Law Enforcement

Law enforcement is the last defense of the State and citizens against banking fraud and scams (New Zealand National Risk Assessment, 2019). Moreover, one of the critical roles in combating fraud should be played by law enforcement agencies and their specialised departments designated to combat financial crimes (Yuhermawa, & Fakrulloh, 2021).

According to Brooks & Button (2011), the main task of law enforcement agencies in the fight against banking fraud and scams is to collect and analyse information from financial industries to conduct active investigations of financial fraud and scams and transfer fraudsters to the judicial
system. However, Cross & Blackshaw (2015) suggests that law enforcement should primarily work with financial institutions, federal banks, and citizens to prevent fraud and scams.

Many scientific articles and studies suggest that law enforcement agencies have more problems than solutions when dealing with fraud and scams (Yuhernawa, & Fakrulloh, 2021). The difficulties associated with accurately assessing financial losses from fraud and scams and the level of victimisation; they pose many challenges for the Police regarding their ability to investigate, prosecute, or arrest fraudsters (Cross, & Blackshaw, 2015). According to Mason & Bohm (2017), for the reasons above, fraud and scam are not a priority for police organisations in many countries due to limited personnel and resources which are usually directed to other more severe types of crime or those who commit crimes where success is faster and easier.

Tracking and investigating banking fraud and scams in connection with virtual and transnational elements of fraud and scams is problematic for law enforcement agencies (Mason, & Bohm, 2017). Offenders use jurisdictional boundaries that prevent law enforcement from investigating and prosecuting (Yuhernawa & Fakrulloh, 2021). Moreover, fraudsters can make several transactions in several countries, making it almost impossible to catch them. Often, a fraudster in one country will target a victim in a second country and request a remittance to a third or even a fourth country. Hence problems arise in determining which police agency has jurisdiction over the matter and who is responsible for investigating and catching the fraudsters (Mason, & Bohm, 2017). Effective interaction between the security forces of different countries and International Police could remedy this situation. Establishing this process requires a tremendous effort from leaders interested in fighting fraud and scams in countries, which is not a priority due to the current realities (Cross, & Blackshaw, 2015).

In addition, from the point of view of the laws of different countries, it is difficult for the police to establish the fact of a fraudulent act and to punish a fraudster since most fraudulent transactions are legally authorised (entering a PIN or using online banking credentials) (Brooks, & Button, 2011).

Based on the above difficulties for law enforcement agencies, the fight against banking fraud and scams on the local-country level comes to the fore (Yuhernawa, & Fakrulloh, 2021). Interaction with federal banks and financial institutions and educational work among citizens is one of the main tasks in reducing the risk of fraud and scam. A well-established system of interaction between citizens and a quick police response when fraud and scams are committed within the country yields tangible results.

According to Mason & Bohm (2017), law enforcement should allocate more funds to modernise information technology and educate police officers in fraud and scam, digital crime.
Mason & Bohm (2017) continues that the state needs to understand that education, training, and provision of the latest technologies for law enforcement agencies is a crucial factor in the fight against banking fraud and scams, and not understanding this fundamental aspect will lead to financial and moral losses on the part of the population and the country.

2.4 Chapter II Summary

The second chapter provided an extensive review and analysis of the existing literature on banking fraud and scams and outlined the theoretical foundations and drew relevant conclusions related to this research. A literature review on banking fraud provided an opportunity to conduct a qualitative and quantitative analysis of the data obtained and propose solutions to the problems of fraud in the subsequent chapters.

The history of the emergence of fraud, evolution, the reasons and factors committing it in ancient times indicate that the psychology of people in terms of committing crimes has not changed much. From time immemorial, people have been driven by three basic instincts when committing fraud: wealth, greed, and need. The reason and factors for committing fraud described in this chapter will help create measures to prevent fraud.

The conducted descriptive analysis of the most common types of banking fraud and scams in world practices will provide an opportunity to identify the most common types of fraud and scams in New Zealand or to reveal new trends in fraud in the New Zealand financial market. Moreover, a deep understanding of the mechanisms for committing fraud and scams will allow the development of several measures to prevent fraudulent encroachments. Familiarising banking services users with fraud and scam types will give people an advantage over fraudsters and avoid financial losses.

Researching the role, successes, and failures of government agencies and financial institutions in the global arena in the fight against financial crimes, coupled with communications with the financial industry professional experts from New Zealand, will identify gaps in the work of the financial industry in the fight against fraud and offer effective solutions based on the best world practices and trends.
CHAPTER III: RESEARCH METHOD

3.1 Introduction

Chapter 3 describes the research design, methodology, approaches, and tools used to conduct this research. Different authors use different terminology to describe how research is conducted, such as methods, paradigms, or approaches. However, experience and results show that it is impossible to use these tools interchangeably or only with each other.

Chapter 3 begins by briefly reviewing the objectives and research questions posed in Chapter 1. The research design (diagrammatic manner) is discussed, followed by the paradigms, approaches, and methodologies. Methods and techniques were used to conduct the research based on world best practices and the researcher’s understanding. Moreover, in Chapter 3, the rationale for this research's paradigms, methodologies, and approaches is provided.

The following sections describe the criteria by which the research participants were formed to conduct the research. Furthermore, this chapter will provide information on how the research tools were created (face-to-face interview and online questionnaire). The final part of Chapter 3 will discuss the ethical standards and considerations.

3.2 Research Questions and Objectives

The key aim of this research was to investigate banking fraud in New Zealand and create a simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud or scams. In addition, the research will help to understand technical aspects and types of bank fraud and scams in New Zealand. Moreover, the research will examine the New Zealand Government and financial institutions' response in the prevention and control of bank fraud, including what has been done until now and what else could be done in the future.

Based on the above, the objectives of this research can be formulated as:

1. To identify the forms of banking fraud and scams in New Zealand.
2. To examine the Government and financial institution's response to the prevention and control of bank fraud in New Zealand, what has been done and what else could have been done.
3. Create a simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud and scams.

To achieve the research goals, it will be necessary to answer the following questions:

1. What are the most common forms of banking fraud and scams in New Zealand?
2. What efforts should the Government (Reserve Bank of New Zealand, New Zealand Police) and financial institutions make to mitigate the risk of fraud for New Zealand citizens?
3. How can the New Zealand community protect itself from banking fraud and scams?

3.3 Research Design

The research design is a detailed outline to achieve the stated objectives and answer the research questions. In contrast, the research plan is a general scheme or programme of research, including all the approaches, methodologies, and tools.

A detailed research design of the research is presented in Figure 15. Figure 15 shows that the research follows the paradigm of Positivism, qualitative and quantitative approaches (mixed methodology). The mixed methods involve face-to-face interviews with banking industry professionals and online questionnaires with the banking services users. The quantitative approach uses descriptive statistics and inferential methods. At the same time, the qualitative approach was used to build hypotheses and draw conclusions based on the triangulation of non-numerical data obtained during the research and the review of open information sources published worldwide. Additionally, the research design plan provides a list of ethical considerations and used research tools.

Figure 15
Research design plan

Note. Research design plan developed by the author.
3.4 Research paradigm

All scientific research and systematic searches for knowledge can be considered through different research paradigms (Alharahsheh & Pius, 2020). Paradigms help make assumptions about how processes and science work in the universe. In essence, paradigms guide scientists and represent the conceptual framework that guides the researcher. Pham (2018) suggests that any paradigm refers to the researcher's worldview, images, and principles of thinking, which affect how they see and analyse the surrounding reality. In other words, the research paradigm is the individual set of principles, methods, and psychological perceptions that influence how the researcher understands reality (Park et al., 2020).

The Positivist Paradigm invites researchers to believe in obtaining reliable data through experimentation to objectively explain reality (Pham, 2018). According to Alharahsheh, & Pius (2020), the Positivist Paradigm uses a deductive form of logic solely; the researcher must generate a hypothesis or theory to test using the information received. This information is collected through interviews or surveys, then analysed using predefined statistical methods (Park, et al., 2020). Based on the analysis, the scientist can conclude. In other words, the Positivism Paradigm is based on genuine and organic evidence that assists to establish causality and uncover objective truth (Alharahsheh & Pius, 2020). However, some scholars criticise the Positivist Paradigm for its inability to analyse natural social phenomena when higher moral and philosophical concepts are involved in the research process (Ryan, 2018). This view suggests that the Positivism Paradigm works well when individual emotions and feelings are not part of the analysis.

On the other hand, Interpretivism is the opposite concept of the research paradigm (Alharahsheh & Pius, 2020). Interpretivism is based on the fact that the researcher must forget about other perceptions of reality and use subjective experience and knowledge to conduct research (Park et al., 2020). Interpretivism uses inductive logic and is based on exchanging information between the researcher and research subjects, which is recorded through conversations, observations, and personal notes (Pham, 2018). However, Interpretivism focuses on accepting personal information and has been criticised for failing to create theories that can be accepted by the majority of the population (Ryan, 2018).

Proceeding from the fact that the researcher will not attempt to interpret the data obtained during the research subjectively, Positivism will be used as the central research paradigm. Moreover, the researcher will use the Paradigm of Positivism to generate hypotheses, literature review, collect
3.5 Research Methodology

Bowen et al., (2017) identify three possible research approaches: quantitative, qualitative, and mixed also suggested that research approaches cannot be viewed as separate classifications; they should be viewed as opposite corners of the same triangle, where research can be conducted using more than one and less of the other approach, so a mixed somewhere in the centre.

This research will rely on a mixed methodology (quantitative and qualitative) to achieve the research aims and answer the three research questions. The mixed methodology involves face-to-face interviews with banking industry professionals and online questionnaires with the banking services users, and the review of open information sources, including scientific articles related to the research topic.

The primary data collection through interviews and the online questionnaire helped the researcher identify the most common types of fraud in New Zealand through conducting a descriptive statistical analysis. This process was followed by collecting secondary research data through the review of existing literature on banking fraud worldwide. Analyse of the collected data to assess common types of banking fraud and identify potential trends (i.e., frequency of incidents, amount of money stolen, and types of misleading potential victims/victims) was undertaken. In addition, possible connections between the information received was established using statistical methods (e.g. cross-tabulation and Chi-square test). The use of existing open data to improve, compare and verify the results of the quantitative analysis was used, where appropriate. Finally, the outcome of this stage informed by the secondary research was used to describe (with examples) the most common types of fraud and scams in New Zealand (the first research question).

To answer the second question, using a similar approach, views of financial industry professional experts and financial industry customers on the government's efforts to mitigate the risk of fraud were collected. The secondary research informed the insights derived from the analysis of collected information. Moreover, possible connections between the data received was established using statistical methods. Finally, the same approach identified ways to protect against banking fraud and scams and create a simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud and scams (the third question).
3.6 Data Collections Tools

Given the nature of the topic, it was decided that the main tools for collecting information would be a face-to-face interview with financial industry professional experts and an online questionnaire with banking services users. Furthermore, these tools are the cheapest, in terms of investment of time and money, methods of collecting information that attracts a large number of research participants. The researcher was convinced that the questions for both instruments were easy to understand, not suggestive, and the choice of answers was mutually exclusive. All questions used minimal financial language that was familiar to any user of banking services.

Before being used on a target group of research participants, both tools were peer-reviewed by the research supervisor and co-supervisor, which helped identify problems and gaps in the tools. Moreover, the researcher conducted pilot testing of the online questionnaire and face-to-face interview with a small select group to identify deficiencies in the tool and rectify these before starting the research. Before the final version was approved, the face-to-face interview and online questionnaire underwent three revisions.

To create an online questionnaire, Google Survey Maker was chosen. This is an online platform specialising in creating any survey and is free. Google Survey Maker offers a two-factor authentication for login with end-to-end data encryption. In addition, it allows storing of the acquired data and extracting tables and graphs in Microsoft Excel. The online questionnaire was also created in Google Survey Maker and has an easy-to-understand user interface. It does not require technical skills on the part of research participants, which helps to eliminate the possibility of losing them.

The face-to-face interview questions with financial industry professional experts were designed to answer research questions and compare them with banking services users. The face-to-face interview with financial industry professional experts were semi-structured and include ten open-answer questions.

The final forms of the research tools can be found in Appendix 1 and Appendix 2. Any answers to the questions from the pilot were excluded from the research.

3.7 Research Participants and Recruitment

The target subjects of this research were the banking services users and products (age older than 18) in New Zealand, regardless of ethnicity and gender. Moreover, to achieve more profound and precise research results, the target group of research participants includes banking industry employees,
which were selected through the researcher's and a co-supervisor's professional network in five major banks of New Zealand.

Financial industry professionals have a deeper understanding of the technological aspects of banking fraud that helped identify the most common types of fraud and scams in New Zealand. While for non-financial industry people, the types of fraud typically remain insufficiently understood, and they only have a general understanding of fraud. Secondly, financial industry professionals are involved in the anti-fraud processes, and their contribution helped understand the specific steps that the Government takes to mitigate the risk of fraudulent activity. However, the opinions, suggestions, and feedback from banking services users about the approach of the Government and financial institutions in the field of combating fraud revealed gaps in the efforts made by the Government and help us identify potential solutions for addressing identified issues. Thirdly, the experience of tackling banking fraud of both groups helped answer the question: "How can the New Zealand community protect itself from banking fraud and scam?" Financial industry professionals know precisely how to avoid becoming a victim of fraud. However, banking services users had specific experiences, insights, and tricks to avoid fraud that professionals from the financial industry cannot efficiently perform. All research participants were able to read and comprehend English on advanced level.

According to the criteria defined and approved by the supervisor and co-supervisor of this research, the researcher identified potential research participants who meet the requirements in different ways as follows:

Financial industry professionals identified from the researcher's (currently an employee of a major New Zealand bank) network and co-supervisor's (a former employee of a major bank in New Zealand) network. In this case, the researcher conducted face-to-face interviews with at least five research participants from the largest New Zealand banks (one research participant from each bank). This approach covered 95% of the New Zealand banking industry (five major banks share a 95% banking market in New Zealand). All identified research participants of the face-to-face interviews were from financial industry professionals in financial crime, cybersecurity, and fraud operations with more than six months of experience and all were invited for the face-to-face interview.

The online questionnaire was been posted via the researchers' professional social networking website (LinkedIn) to invite banking services users to participate, providing a random group of research participants. One-hundred and ten online questionnaire responses were analysed using the previously described methodology quantitatively. Before undertaking the face-to-face interview or the online questionnaire, each research participant (banking industry expert or banking services user) was provided an explanatory information sheet about the purpose of the research with an invitation to
fill out an online questionnaire for banking services users or participate in a face-to-face interview for financial industry professional experts. Besides, all research participants signed informed Consent. The face-to-face interview or online questionnaire were conducted voluntarily, and a research participant could deny an invitation without explanation. The face-to-face interview or online questionnaire included different types of questions: open, closed, and multiple-choice.

### 3.8 Data Collection

During the online questionnaire with banking services users, data collection was carried out at randomly and was aimed at the fact that the research participant was a user of banking services (has valid accounts and bank cards). Five research participants that undertook the face-to-face interview were selected from the personal connections of the researcher and the co-supervisor of the research.

A systematic approach was undertaken for the data collection phase, which lasted approximately three months from June 2021 to September 2021. Data collection included the following sub-steps:

(i) creating research tools;
(ii) determining a sample of research participants and searching for them;
(iii) conducting research using the developed tools;
(iv) administration and retrieval of data.

After five financial industry professionals experts were identified, formal email invitations were sent to them explaining the research's objectives. While, to obtain the desired number of responses to the online questionnaire, the researcher established relationships with potential research participants and published a uniform resource locator (URL) address explaining the survey's objectives through the professional social media website, LinkedIn. If a potential research participant agreed to undertake the online questionnaire, then the research participant clicked on the URL address, which redirected them to the secure and Cloud-based tool called Google Survey.

Google Survey is an administrative platform that offers a wide range of tools for conducting research and creating research tools. Moreover, Google Survey has many functions for grouping, organising, and analysing the information obtained during the research, which helped the researcher to simplify the process and obtain various reports and graphs online. The services offered by the platform are free and reduce the psychological burden on the researcher and reduce the risk of human error, especially when performing calculations and charting. To create the online questionnaire tool,
the researcher used simple questionnaire forms with open, closed, and multiple-choice questions templates included in advance.

As the research participant answered the online questionnaire, their status and progress was updated automatically. If one or more questions were not answered, the research participant received a notification about this, although there were no mandatory questions in the online questionnaire. After completing the online questionnaire, the research participant was invited to leave a personal email to receive a copy of the research, this was optional. Google Survey Maker provided information to the researcher about how many online questionnaires had been completed since publication in automatic mode. This feature helped the researcher monitor the progress of data collection in an automated manner.

The researcher applied the data collection process via the LinkedIn website. Figure 16 provides a detailed plan of the data collection process via LinkedIn. In case of any questions, the researcher used LinkedIn chat to interact with potential research participants and research participants of the online questionnaire. Following LinkedIn's security policy, the researcher could not send messages to potential research participants if both parties did not agree on the connection. For this reason, the researcher sent a request to establish a relationship, obtained the consent of a potential research participant, and then offered to participate in the research.

**Figure 16**

Online questionnaire data collection process

Note. Online questionnaire data collection process developed by the author.
To achieve the 110 completed online questionnaire, the researcher sent 15 requests to join and participate in the research every day during 2 months, introducing himself and sharing his intentions. The researcher considered that if the potential research participant accepted the connection request, they would be ready for the next step. After obtaining consent, the researcher sent a "Thank you" message and presented the research. If a potential research participant responded and showed interest, the researcher sent the hyperlink to participate in the research with instructions and a preamble. The researcher waited three days for consent to confirm the connection or to go through the online questionnaire. If the researcher did not receive any communication from the potential research participant within six days (in total), the researcher stopped further attempts to contact the research participant. After completing the online questionnaire, the researcher sent a "Thank You" message to the research participant and after they received an automatic confirmation from the Google Survey platform that the research participant had completed the online questionnaire.

The data collection process from the financial industry professional experts was more straightforward and did not require schemes. The researcher found research participants for the face-to-face interview via personal and co-supervisor connections. At the first stage of involving financial industry professional experts in the face-to-face interview, a verbal agreement with potential research participants was carried out. After that, the researcher sent an email to each research participant with interview questions. The research participant received the face-to-face interview questions one week before the interview, which helped them prepare in advance. Subject to COVID-19 restrictions, all face-to-face interviews were conducted online using the Microsoft Teams platform.

### 3.9 Data Analysis

Data analysis can follow a linear approach that assists the researcher with ease of use by using a predefined process that is simple and structured (Muna, 2020). However, Kaur et al., (2018) suggest that data is usually disorganised and complex. Hence, researchers need to use more than one way to analyse the data and be prepared to change analysis methods as new variables appear during the analysis. Therefore, the researcher decided to use two forms of quantitative research - descriptive, and inferential (Shorten & Smith, 2017).

To achieve the objectives of the research, the researcher began analysing the data with descriptive analysis. According to Muna (2020), descriptive analysis helps to provide data in a generalised form. Moreover, descriptive analysis helped to provide an overview of the characteristics of the dataset and provided opportunities for more in-depth exploration. Kaur et al., (2018) suggest
using descriptive analysis early in the investigation to formulate a common understanding of the findings, accept or refute judgments and hypotheses, and continue further research. The resulting data provided a wealth of information about the various parameters of a dataset. However, descriptive analysis helped the researcher understand which measurements would be helpful for further research and which was discarded (Mishra et al., 2019). The researcher used inferential analysis to draw properties of probability distributions for formulating and testing hypotheses. The inferential analysis used data from predetermined sample sizes, predicted probabilities in larger populations, and took the form of null hypothesis significance tests.

In the first stage of data analysis, the descriptive analysis were employed to answer the first two research questions:

1. What are the most common forms of banking fraud and scams in New Zealand?
2. What efforts should the government (Reserve Bank of New Zealand, New Zealand Police) and financial institutions make to mitigate the risk of fraud for New Zealand citizens?

The raw non-numerical data was encoded with nominal values, and then the encoded data was analysed using Microsoft Excel pivot tables, descriptive statistics functions, and visualisation. After receiving the processed data and visualising, the researcher generated hypotheses and tested them in the following analysis phase. To test hypotheses, the researcher used cross-tabulation and applied the Chi-square method to find the p-values and assess them to accept or reject null hypotheses. Alavi & Cleary (2020) suggest using the Chi-square test to correlate categorical variables to provide complete answers to the questions posed and draw key research findings. For instance, whether the Government is making enough efforts to reduce the risk of banking fraud (Yes / No) or whether people know how to protect against banking fraud (Yes / No). In conjunction with the literature review, the results of hypothesis testing and the relationship between the obtained data assisted to answer all the research questions and achieve research aims.

3.10 Ethical Considerations

This research was conducted under the Otago Polytechnic Auckland International Campus (OPAIC) policy and the Otago Polytechnic Research and Ethics Committee. The researcher submitted two applications to the OPAIC Research and Ethics Committee: a research proposal and an ethics application; both were approved. The Whakapapa Māori fundamental principles were considered during the entire research, where appropriate. The researcher consulted with a Māori professional to ensure that the Māori research ethics were met. The research used all the Whakapapa Māori principles,
which allowed the research to be conducted following the cultural, spiritual, and material values of Māori. This approach benefited the whanau, iwi, hapu, and the entire New Zealand community.

In the course of the research, there were risks indented that may have undermined the confidentiality of the researcher and research participants' data which may have caused harm to their well-being and health. For this reason, the researcher took the following steps to address these:

1. Privacy: The identity of the research participants of the online questionnaire remained anonymous. There was no option even for the researcher to identify which research participant provided what answers for the online questionnaire. However, the identity of the face-to-face interview research participant was only known to the researcher (only financial industry professionals with relevant experience in the banking sector were identified and recruited), and no record was kept due to sensitive information of banking industry and personal data protection.

2. Data Security: All data obtained during the research was stored on secure computers and will be held securely on external backup storage for seven years in compliance with the Otago Polytechnics Policy. The researcher chose a tool (Google Survey) with two-factor authentication and end-to-end data encryption for the research which protected gathered data from unauthorized access.

3. Informed Consent: Before the online questionnaire or face-to-face interview, each potential research participant (financial industry professional expert or banking services user) was given an explanation about the purpose of the research with an invitation to fill out the online questionnaire for banking services users or participate in a face-to-face interview for financial industry professional experts. The online questionnaire or the face-to-face interview was been conducted voluntarily, and a potential research participant could deny an invitation without explanation.

4. Vulnerability: No potential vulnerabilities to the banking services users were identified since the online questionnaire is conducted online. Each research participant could answer the questionnaire at any convenient place and period of time. There is no time limit for the online questionnaire. The online questionnaire consisted of ten close, open, and multiple-choice questions. The face-to-face interview with financial industry professional experts was semi-structured and include ten open-answer questions. The interviews were conducted out of working hours, and research participants decided the time, date, and place. To avoid the vulnerability of all research participants, they could refuse to participate in the research at any stage or skip any question if they did not want to answer without explaining. Furthermore, all research participants received an explanation about the main topic and aims of the research before taking part in the research. The first part of the online questionnaire was a short paragraph which included information about research aims.
To motivate research participants (banking services users) to take part in the online questionnaire, they were provided the information about the seriousness of the fraud problem in the banking sector worldwide and in New Zealand in particular (the short paragraph at the begging of the online questionnaire). It explained to research participants that their contribution to the research would help reduce the level of fraud in the banking sector and improve the well-being of the New Zealand community. Moreover, the researcher offered a copy of the research results to every research participant upon completion (optional). The research participants received copies all findings of the research, especially the simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud and scams.

3.11 Chapter Summary

The researcher decided to use the Positivism Paradigm as the primary paradigm to answer the research questions and achieve the goals raised in Chapter 1. Furthermore, the researcher used a mixed methodology (quantitative and qualitative) to complete the research aims and answer the three research questions. The mixed methodology involved online questionnaires with the banking services users and face-to-face interviews with financial industry professional experts and a review of open information sources related to the research topic and analysing the data by using two forms of quantitative analysis - descriptive, and inferential.

Given the nature of the topic, the researcher decided that the main tools for collecting information would be a face-to-face interview (Appendix 1) with financial industry professional experts and an online questionnaire (Appendix 2) with banking services users. The online platform Google Survey Maker was been chosen to create the online questionnaire. The face-to-face interview questions with financial industry professional experts were designed to answer research questions and these were then compared with banking services users. The face-to-face interviews with financial industry professional experts were semi-structured and included ten open-answer questions.

To obtain the desired number of responses to the online questionnaire, the researcher established relationships with potential research participants and published a URL address explaining the objectives of the questionnaire through the professional social media website LinkedIn. For the face-to-face interviews, all research participants were identified via the researcher and co-supervisor personal connections and recommendations.
Finally, the research was conducted under the Otago Polytechnic Auckland International Campus policy, the Otago Polytechnic Research and Ethics Committee, whakapapa principles, and Māori values.
CHAPTER IV: ANALYSIS

4.1 Introduction

Chapter 4 provides a detailed analysis of the data obtained. As discussed in Chapter 3, to achieve the research objectives, the researcher decided to use The Positivism Paradigm and the two forms of quantitative data analysis, descriptive, and inferential analysis.

Moreover, in the following sections of Chapter 4, the background history of the data, the appropriate steps to remove noise and unnecessary information from the data will be articulated.

4.2 Datasets

The researcher used two datasets from the online questionnaire and the face-to-face interview for the analysis.

The two datasets from the online questionnaire and the face-to-face interview were analysed.

One hundred and thirteen banking services users undertook the online questionnaire. The respondents answered 13 questions of various types: open, close, and multiple-choice. Thus, the row dataset includes 14 columns and 113 strings (contains names of columns). Figure 17 shows the raw dataset from the online questionnaire, this was downloaded from the Google Survey platform.

Figure 17

Online questionnaire data set (fragment)

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Time stamp</td>
<td>How do you rate your</td>
<td>Which forms below of</td>
<td>Has somebody attempt</td>
<td>If you answered “Yes”</td>
<td>7. Have you ever been</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>02.07.2021 11:01:15</td>
<td>b) Highly familiar</td>
<td>a) Romance - a confident</td>
<td>Yes</td>
<td>123 b) No</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>3</td>
<td>02.07.2021 11:04:17</td>
<td>a) Highly familiar</td>
<td>a) Romance - a confident</td>
<td>Yes</td>
<td>Quiet b) No</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>15.07.2021 17:19:35</td>
<td>b) Fairly familiar</td>
<td>a) Romance - a confident</td>
<td>Yes</td>
<td>Skimming - an illegal; c) I do not know b) No</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>15.07.2021 17:19:53</td>
<td>b) Fairly familiar</td>
<td>a) Romance - a confident</td>
<td>Yes</td>
<td>Emails, text messages, p) Yes</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>6</td>
<td>15.07.2021 17:20:42</td>
<td>b) Fairly familiar</td>
<td>a) Romance - a confident</td>
<td>Yes</td>
<td>My friend’s social media e) Yes</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>7</td>
<td>15.07.2021 17:48:33</td>
<td>a) Highly familiar</td>
<td>a) Romance - a confident</td>
<td>Yes</td>
<td>The most frequent ones b) No</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>8</td>
<td>15.07.2021 18:10:05</td>
<td>b) Fairly familiar</td>
<td>a) Romance - a confident</td>
<td>Yes</td>
<td>b) No</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>9</td>
<td>15.07.2021 18:16:59</td>
<td>c) Not much familiar</td>
<td>c) I do not know</td>
<td>b) No</td>
<td></td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>10</td>
<td>15.07.2021 18:24:16</td>
<td>a) Highly familiar</td>
<td>f) Phishing - a type of soi</td>
<td>b) No</td>
<td></td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>11</td>
<td>15.07.2021 18:30:44</td>
<td>b) Fairly familiar</td>
<td>a) Romance - a confident</td>
<td>c) I do not know</td>
<td>b) No</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>12</td>
<td>15.07.2021 18:40:21</td>
<td>c) Not much familiar</td>
<td>h) Other</td>
<td>a) Yes</td>
<td>Fraudulent transactions e) Yes</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>13</td>
<td>15.07.2021 18:40:29</td>
<td>c) Not much familiar</td>
<td>a) Romance - a confident</td>
<td>c) I do not know</td>
<td>b) No</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>14</td>
<td>15.07.2021 18:49:47</td>
<td>c) Not much familiar</td>
<td>c) Skimming - an illegal; a) Yes</td>
<td>b) No</td>
<td></td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>15</td>
<td>15.07.2021 18:51:54</td>
<td>a) Highly familiar</td>
<td>a) Romance - a confident</td>
<td>b) No</td>
<td>Phishing emails</td>
<td>c) I do not know</td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>16</td>
<td>15.07.2021 19:06:47</td>
<td>b) Fairly familiar</td>
<td>b) Investment - a deceptive</td>
<td>a) Yes</td>
<td>Steal my card number (p) e) Yes</td>
<td></td>
<td></td>
<td>123</td>
<td>28</td>
<td>14</td>
<td>18</td>
<td>17</td>
<td>14</td>
<td>18</td>
<td>17</td>
</tr>
</tbody>
</table>

However, the dataset obtained from face-to-face interviews with financial industry professional experts is not tabular and consisted of ten open-ended questions from each research
participant. Five face-to-face interviews were conducted with financial industry professional experts from four of the largest banks in New Zealand, and one research participant was from a large cybersecurity company. With the permission of the research participants, the researcher recorded the answers to the questions using the voice recorder built into the Microsoft Teams app.

4.3 Data pre-processing

When conducting any data analysis, the first step towards achieving the desired result is to prepare the obtained data for calculations and analysis’ includes clearing the dataset of missing values, clearing up various noise or cells that the research participants filled in incorrectly. The dataset preparation process helped to avoid calculation errors and incorrect analysis.

At the first stage of dataset preparation, the researcher copied the dataset from the Google Survey Maker platform to Microsoft Excel. Microsoft Excel included a set of essential formulas and graphs that simplified the analysis. To conduct this research, the researcher needed all columns and strings except for the "time" column (Figure 17), which meant the time it takes for research participants to complete the online questionnaire. The researcher removed the column “time” as unnecessary.

At the next dataset preparation stage, the researcher applied a system of filters to the resulting table. This function reduced the time spent on sampling and plotting. The researcher corrected the grammatical errors made by the research participants and filled in empty cells manually or using the Microsoft Excel filter system. Figure 18 shows a dataset ready for analysis in tabular form (fragment).
4.4 Descriptive Analysis

In this section of the research, the researcher discusses the results found during the descriptive analysis. The descriptive analysis helped generate the hypotheses and some parts of the conclusions and prepare the research for further analysis (inferential). Moreover, the descriptive analysis assisted in the preparation of robust arguments to achieve the research objectives.

At the first stage of the descriptive analysis, the researcher realised that the prepared dataset contained many valuable non-numerical data, which could not be used for calculations since all types of qualitative research is only possible using with numerical data. For this reason, the researcher coded all non-numerical data, numbered for all options in every online questionnaire that required it. In other words, since the answers were categorical and did not involve the use of numbers, the researcher assigned them numerical values. The assignment of numerical values for categorical data was completed by assigning a specific number to each answer. For instance, for the options for answering the question “How many years have you been using banking services in New Zealand?”, the number
“1” was assigned to the option “one-three years”, the number “2” was assigned to the option “four-six years”, the number “3” was assigned to option “seven-ten years” and so on. The researcher used the same way to assign numerical data for the 11 answers to the online questionnaire. Since the online questionnaire contains 11 questions and 113 answers (1243 variables), the researcher decided to use the Microsoft Excel “IF” classification formula. For example, the “IF” formula for the first question of the online questionnaire looks like this:

```
=IF(A7="1-3","1";IF(A7="4-6","2";IF(A7="7-10","3";IF(A7="10-15","4";IF(A7="more than 15","5")))))
```

The researcher applied a similar approach to all answers for 11 questions requiring data processing.

For a more convenient and visualised display of the results of the descriptive analysis, the researcher used Microsoft Excel pivot table and visualisation tools. Microsoft Excel tables and plots assisted the researcher to perform exploratory data analysis and formulate hypotheses for testing and identifying possible relationships between various variables. Furthermore, the researcher used descriptive analysis to understand the findings and assess what other analysis needed to be performed to answer the research questions.

### 4.4.1 Customer’s and Experts Banking Experience

In this sub-section, the researcher analysed the individual characteristics of the research participants in the online questionnaire and the face-to-face interview. Figure 19 shows how many years (experience) of research participants in the online questionnaire have used banking services in New Zealand.
All research participants (N = 113) of the online questionnaire responded to the question: How many years have you been using banking services in New Zealand? According to Figure 19, the banking experience fell into five categories; 25.5% of research participants have little experience using banking services - from one to three years (n = 29), 25% have experience from four to six years (n = 28); only 5% have experience from seven to ten years (n = 6). Approximately 14% of the research participants have experience from seven to 15 years (n = 16), 30% have more than 15 years of experience in using banking services (n = 34). Based on the data obtained, it can be concluded that about 50% of the research participants in the online questionnaire were experienced banking services users, having more than seven years of experience.

As for the experience of financial industry professional experts, all research participants in the face-to-face interviews have more than six months of experience in financial crime, fraud operations, and cybersecurity industries, which makes them financial industry professional experts and allowed them to take part in face-to-face interviews.

### 4.4.2 Familiarity and Knowledge about Fraud and Scam

This sub-section covers the research participant’s knowledge and familiarity with banking fraud and scams. It allowed the researcher to understand how much the research participants understood and know about the common types of banking fraud and scams, as well as opinions on the most common types of fraud in scams in New Zealand.
4.4.2.1 Familiarity

The online questionnaire asked research participants: How do you rate your familiarity with different forms of the most common scam in New Zealand? All research participants provided an answer to the question. Figure 20 below shows the breakdown of the familiarity of banking services users with fraud and scams.

Figure 20
Familiarity of banking services users with fraud and scams in New Zealand

Figure 20 shows that 20% (n = 23) were unfamiliar with banking fraud types. However, other research participants had a reasonable understanding of banking fraud and scams, 22% (n = 25) were highly familiar, and 58% (n = 65) are fairly familiar.

4.4.2.2 Fraud and Scams Typology Knowledge

To answer the question about knowledge and understanding of certain types of banking fraud and scams, the research participants of the online questionnaire were offered eight answer options with the ability to choose as many options as they wanted. The last response option - "Other" asked research participants to indicate other fraud and scams they were aware of. Figure 21 shows the breakdown of banking services users ’ knowledge about types of fraud and scams.
According to Figure 21, all the types of banking fraud and scams in the online questionnaire were familiar to at least 50% of the research participants (the lowest response - investment scam n = 58). The most common type of fraud among those responding to the online questionnaire was phishing, as 83% (n = 93) mentioned phishing. Skimming, identity theft, and lottery scams (83, 85, and 84 research participant mentions, respectively) received approximately (75%) an equal number. The invoice scam was selected by 70 (62.5%) research participants. Romance and investment scams had the lowest responses among the suggested answer options (61 and 58 research participant mentions, respectively). Nine research participants provide other types of fraud and scams. Seven research participants (6%) mentioned phone call scams.

However, the financial industry professional experts’ answers show a slightly different picture than banking services users’ answers. Figure 22 shows the most common types of banking fraud and scams in New Zealand.
Figure 21

The most common types of banking fraud and scams (according to experts' opinion)

All financial industry professional experts were convinced that the most common types of banking fraud and scams in New Zealand were phishing and romance scams. Furthermore, 80% of financial industry professional experts mentioned investment scams. A comparison of Figure 21 and Figure 22 suggests that the phishing scam was most familiar to banking services users and is also the most common in New Zealand. However, romance and investment scams, which are also common (according to financial industry professional experts) in New Zealand, were not the most familiar among banking services users. Moreover, according to Chapter II and the Netsafe Report (2021), they are the most common types of scams reported by the New Zealand community.

The lack of knowledge and understanding of the types of fraud by banking services users may be the root cause of the high rate of these types of fraud.

4.4.3 Fraud Attempts and Victims

To answer question 5: “Has somebody attempted to commit banking fraud or scam on you?” the research participants of the online questionnaire were offered three answer options – "yes, no, or I do not know", with the ability to choose only one option. Figure 22 shows the number of banking services users which fraudsters tried to commit fraud and scams. Approximately 50% of the research participants \( (n = 56) \) were sure that the fraudsters tried to commit fraudulent actions on them and steal money. However, 32% of research participants \( (n = 36) \) in the online questionnaire believe that no one has ever tried to deceive them. At the same time, 18% of the research participants \( (n = 21) \) do not know or are unsure about their involvement in fraudulent events.
The next question, the online questionnaire, was open and asked the research participants to name the type of fraud or scam that the fraudsters tried to commit. If the research participant was unsure about the accuracy of the terminology or the type of fraud, they were asked to describe the actions that the fraudsters tried to commit.

In this case, the researcher removed 36 research participants from this part of analysis because they were confident that there was no fraudulent attempt on them. However, the researcher decided to keep the total number of research participants in the plotted graphs to display more information. Only 6% (n = 5) provided the name of the type of fraud or scam. The researcher manually studied the answers of the rest of the research participants responses and identified the types of fraud. The researcher was unable to locate some descriptions of the types of fraud due to vagueness and inaccuracy. The researcher assigned the vague answers to the category "I do not know."

Figure 23 shows the distribution of responses from research participants in the online questionnaire by the type of fraud and scam in which they believe they were involved.
According to Figure 23, phishing was the most popular type of scam. Phishing was identified and described by 33% (n = 26) involved in fraudulent events. Not one research participant named BIN-attack. However, based on the descriptions of the fraudulent events provided, the researcher was able to identify a BIN attack for 10% (n = 8) of the research participants. Another type of fraud with bank cards - skimming was determined by 5% of research participants. The third most popular category was the investment scam. Six percent (n = 5) of the research participants identified this type of scam. The smallest number of responses scored identity theft, invoice scam, and phone call scam (3, 1, and 3 research participants, respectively).

However, 35% (n =27) of the research participants could not identify the type of fraud or provide a clear description. This information may indicate that the category of research participants who could not identify fraud is highly likely to fall into fraud and scam.

Question 7 asked research participants if they had ever been victims of banking fraud and scams. This question was of a closed type and offered the research participants three answers – yes, no, I do not now. Figure 24 shows the distribution of responses from banking services users.
Figure 24
Number of banking services users who have fallen victim to banking fraud and scams

According to Figure 24, only 24% (n = 27) of the research participants were victims of banking fraud or scams. While slightly over 71% (n = 81) of research participants have never been a victim. A minor group (n = 5) is unsure if they have fallen victim into banking fraud and scam.

When conducting a comparative analysis of the number of fraud attempts and the amount of fraud committed, the researcher noticed that not all attempts were successful for the fraudsters. Namely, among 56 attempts, only 27 were successful and resulted in financial losses for the research participants. Based on the above, it can be assumed that more than 50% of the online questionnaire research participants avoided being scammed for one reason or another.

4.4.4 Government and Financial Institutions Involvement

4.4.4.1 Victim Support from Government and Banks

Question 8, in the online questionnaire, asked research participants who were victims of banking fraud and scams, whether they received support from the Government or financial institutions. For this reason, only 27 (100% of fraud victims) provided answers to the question. This question was open-ended and assumed that the research participants would describe the type of support they received from the Government or financial institutions. Figure 25 shows the distribution of banking services users who received or did not receive support from the government or financial institutions after falling victim to banking fraud and scams.
According to Figure 25, 70% of participants (n = 19) received support after falling victim to banking fraud and scams. However, 30% (n = 8) have not received anything. All research participants who provided a more detailed answer to this question noted that they received support only from the financial institution, and no one noted support from the Government. However, seven victims mentioned that they reported to the police via the official New Zealand Police website, and they received only automatic responses. All research participants left similar comments: "The bank cut off my accounts and eventually (after they investigated) I got a full refund"; "Yes, the bank and Visa helped me out and I get my money back"; "Credit card reader on an ATM in Auckland. The bank reimbursed the money that was fraudulently spent"; “I contacted the bank to cancel my debit card. The transactions I pointed out as fraudulent were reversed, and I got my money back within a few weeks”.

Thus, it seems that the financial institutions’ support consists of replacing bank cards or restoring access to online banking, immediately informing the user about the incident, and refunding the stolen funds, which is an essential attribute for banking services users. However, the listed measures above are the solution to a problem that has already occurred and does not prevent or mitigate the risk of banking fraud and scams in any way.

4.4.4.2 Opinions about Government and Banks Involvement

4.4.4.2.1 Banks Involvement

The online questionnaire's ninth question asked banking services users whether the bank they use could protect them from banking fraud and scams. This question was closed-ended and suggested
three answer options (yes, no, I do not know) with the ability to choose one option. All research participants provided an answer to this question. Figure 26 shows the distribution of research participants’ answers about their banks’ ability to protect customers from fraud.

**Figure 26**
Bank's ability to protect customers from fraud and scams (customer’s opinion)

![Bar chart showing the distribution of responses](chart.png)

According to Figure 26, more than half (54% (n = 61) of all research participants in the online questionnaire were confident that the bank they use could protect them from banking fraud and scams. A small number of research participants (60% (n = 18) believe banks could not protect their banking services users from fraud and scams. The rest of the research participants (30% (n = 34) were not exactly sure about the ability of their banks to protect their banking services users and provided the answer "I do not know".

However, five financial industry professional experts admitted that the banking system is not fully capable of protecting customers from fraud and scam, and is far from perfect. According to four interviewed financial industry professional experts, financial institutions can detect suspicious bank card transactions and decline or block them if necessary. However, these are usually based on emerging fraud trends and historical data points. New fraud typologies require data to support patterns for systems to be updated with the latest techniques used. They currently never seems to be a perfect solution for detecting suspicious transactions without identifying some incorrectly flagged genuine transactions (false positives).

Furthermore, online banking seems to be at a technological disadvantage. There is currently no technological means to actively block a suspicious online transaction and no preventative measures that can be enacted if the transaction goes through, e.g., holding funds in a recipient account without
manual analyst intervention. The online system itself is currently outdated and what many transactions would be flagged as suspicious based on historical precedence are not suspicious in the modern-day, which results in a lot more genuine transactions being brought to the attention of analysts. Due to all these factors, protecting banking services users against fraud and scams through online banking is doable but infinitely harder for the financial institutions themselves.

To answer the following question in the online questionnaire, the research participants had to compare the protection banks provide (if they use more than one bank) against fraud and scam. This question was open and assumed that the research participants would share their life experiences and feelings. However, only 23% (n = 26) shared their experiences. Figure 27 shows the distribution of banking services users' answers about different banks' levels of protection against fraud and scams.

**Figure 27**
Difference between New Zealand bank's level of protection against fraud and scams

According to Figure 27, most research participants - 81% (n = 21) who answered this question and shared their experiences say that New Zealand banks provide the same level of security to their banking services users. However, 19% (n = 5) reported different levels of protection and provided specific examples. For instance, "my family and I use a few banks but only bank XXX and does a good job at protecting our accounts. At the beginning of this year my husband accidentally almost bought an expensive phone from company XXXX (wanted to check the shipping fees), and XXX blocked the payment since it was quite an unusual behaviour of my husband. Therefore, they assumed the bank card was stolen or lost and blocked it straight away. He got a new bank card within a week". To maintain privacy, the researcher removed the names of the bank and company.
4.4.4.2.2 Government Involvement

The online questionnaire's eleventh question asked banking services users if they saw the New Zealand government was taking action to mitigate the risk of banking fraud and scams. This question asked research participants to choose one answer out of three: yes (New Zealand Government participation), no (New Zealand Government participation), and I do not know. All research participants provided an answer to the question. Figure 28 shows banking services user’s perceptions about the New Zealand Government's involvement in fraud mitigating processes.

**Figure 28**

Banking services users feel New Zealand government involvement in fraud mitigating process

According to Figure 28, the minority of research participants (around 12% (n = 12) research participants) perceived that the New Zealand Government was participating in mitigating the risk of banking fraud and scams. Slightly over 30% (n = 35) of research participants perceived that the New Zealand government does not participate in the mitigating of risk of banking fraud and scams. However, most research participants (over 56% (n = 64) are not sure that the New Zealand government is participating in the mitigating of risk of banking fraud and scams. In this context, the answers "I do not know" may mean that research participants did not know if the Government was participating in the mitigation of risk of banking fraud or scams. This answer can be equated to “No” (in some cases). On top of that, five out of five financial industry professional experts mentioned that Government involvement is poor in the mitigating of risk of banking fraud and scams and requires improvement.
4.4.4.3 Government and Banks Actions against Fraud and Scams

The twelfth question, the online questionnaire, asked banking services users what measures financial institutions and the New Zealand Government could take to reduce the risk of banking fraud and scams. The question suggested that research participants in the research would share their experiences. All research participants provided an answer to this question. The researcher manually analysed all the responses and assigned a specific category (depending on what the research participants suggested). Figure 29 shows what actions the research participants suggested in the online questionnaire.

**Figure 29**
What measures the government and banks should take to mitigate the risk of banking fraud and scams (banking services users’ opinion).

![Figure 29: Bar chart showing the number of responses for different measures. The y-axis represents the number of answers, ranging from 0 to 60. The x-axis lists various measures: Collaboration with banks, Cybersecurity, Education citizens, I do not know, Laws - strong punishment, Only banks can protect, Police development, They cannot. The chart shows that the largest number of answers (57) is for the option 'I do not know'.]

According to Figure 29, most research participants (around 50% (n = 57)) did not provide any particular suggestion about the measures that the New Zealand Government and financial institutes could take to mitigate the risk of fraud and scams (I do not know). However, slightly under 24% (n = 27) said that educating from primary school to senior citizens would reduce the risk of fraud. For instance, research participant's responses included the following:

1. Extend a school program and teach intermediate school pupils to detect fraud and avoid it.
2. Provide free meetings/get together for communities and teach citizens how to recognise financial frauds, especially for older people.

Moreover, all financial industry professional experts mentioned that the most effective anti-fraud measure is the awareness and educating of banking services users. Financial industry
professional experts believe that the Government and financial institutions need to work together to introduce educational programs in schools and institutes and disseminate information about fraud and scams through social media and on high-rated television channels and radio.

The second most popular measure among banking services users is the strengthening of cybersecurity by banks and the Government (7% \((n = 8)\). Slightly under 7% of the research participants \((n = 7)\) believe that the New Zealand Government could review fraud's legal framework and liability. For example, the responses to the question contained the following comments: "Better tracking people who fraud and scam and put them in jail; stricter punishments". Furthermore, financial industry professional experts said New Zealand's banking fraud and cybercrime laws are lenient and do not provide severe penalties even for repeated violations. Financial industry professional experts believe it was necessary to toughen the punishment for committing fraud, especially for persons of the accounts which the fraudsters transfer the stolen funds (pawns or mules). Mules are a critical part of the bank fraud and scam ecosystem. By eliminating mules, the Government could significantly reduce cybercrime. Currently, there is no penalty for aiding fraud or scams under New Zealand law.

A small number of the online questionnaire research participants (4\% \((n = 5)\)) believe that only banks can protect their customers, and Government involvement is not required. Slightly under 4\% \((n = 4)\) say that only close interaction between Government and financial institutions can resist fraud and scams. Besides, financial industry professional experts believe better collaboration between banks, law enforcement, and the Government is needed to help minimise the potentially devastating impact fraud and scams have on the financial wellbeing of victims. According to financial industry professional experts, the key to the success of this measure is information sharing between all stakeholders.

A minority of research participants (over 1\%) mentioned customer insurance and New Zealand police reinforcement measures. However, four out of five financial industry professional experts said the Police need modernisation. The New Zealand Police needs more human and technological resources to help them to gather evidence against national facilitators of fraud and scams. The New Zealand Police often do not have the resources to build comprehensive cases to maximise punishment.

### 4.4.5 Insights to Mitigate Fraud and Scams

#### 4.4.5.1 Banking Services User’s Insights

The online questionnaire's last question asked a banking services user about the anti-fraud protection they use in their daily lives. The researcher manually analysed all the proposals of the
research participants. The researcher divided all proposals into categories based on the proposed anti-fraud methods. Respondents who did not provide an answer to this question were categorized as “I do not know”. Figure 30 below outlines how banking services users protect themselves from banking fraud and scams.

**Figure 30**
Banking services user’s insights against fraud and scam

![Bar chart showing the number of suggestions in different categories](image)

According to Figure 30, most research participants (slightly under 50% (n= 55)) prefer to use behavioural defenses. According to banking services users, behavioral safeguards include the following points:

1. Do not discuss personal information with strangers or representatives of any companies, including ID, bank card data, and online banking.
2. Do not click on links in received text messages and emails - immediately delete received correspondence from unknown and unexpected sources.
3. Do not make a quick decision about spending (investing). Take a breath, think, discuss with partners and friends, and ask a specialist or community before, collect feedback.
4. Regularly change passwords for the accounts and do not save passwords in the history of Internet browsers.
5. Do not answer phone calls from unknown numbers. Block incoming phone calls from unknown numbers.
6. Be mindful, especially about purchases on investments through the Internet – it is too good to be the truth.
7. Make sure that the call was coming from an actual company by asking them to send an email or mail with the confirmation of what is happening, make a call to the company and ask them if they called you.

8. In case of being scammed, separate funds across several accounts.

The minority of research participants 5% (n = 7) believe that only the government and financial institutions can protect the country's citizens from banking fraud and scams. Research participants who fall into the "institutes" category name such methods of struggle as spreading information about fraud and scams through social media, strengthening the cybersecurity of banks and government institutions, and introducing a fraud-related educational system among the community. However, 1% of research participants (n = 2 prefer to use technological techniques such as antivirus and licensed software.

4.4.5.2 Experts Insights

The last question from the face-to-face interviews with the financial industry professional experts was as follows: “What methods and technologies can you advise banking services users to avoid fraud (share your experience and best practices)?” All the research participants in the face-to-face interview provided detailed answers to the question. After a deep analysis of the information received, the researcher was able to identify only behavioural techniques for combating banking fraud and scams. Moreover, insights received from banking services users and from financial industry professional experts in the financial industry were very similar but not the same. Experience in combating fraud and scams allowed financial industry professional experts to provide more detailed approaches and methods to reducing the risk of fraud and scams.

In addition, some financial industry professional experts (n = 3) noted that technological protection methods played a secondary role for banking services users due to their high price and social engineering presence. The majority of banking fraud and scams are committed based on misleading or deceiving the victim, which is, using social engineering. Fraudsters are excellent psychologists and communicators. For this reason, financial industry professional experts believe that morale, emotion control, and awareness among banking services users play a crucial role in countering fraud and scams.

Financial industry professional experts have suggested the following behaviour for banking services users:
1. If a banking services user receives a suspicious text, phone call or email, question its authenticity by going directly to the source, either in person or by calling their listed phone number as found in an open-source Internet search. For example, if a banking services user receives a phone call from a bank, be polite, hang up, find the genuine phone number of the contact centre through the Internet, make a call and clarify what happened.

2. Talk to professionals, and collect feedback from different sources before choosing to invest in anything – this may cost money. At least a banking services user will have the security of their financial advice to fall back on rather than being scammed easily. The New Zealand government agency – FMA website contains a complete list of genuine and fraudulent merchants related to any investment opportunities.

3. Avoid clicking on any links in emails or text messages from a bank or other companies – go to the sender's official website or make a call.

4. Use passwords with very high entropy containing uppercase and lowercase letters, symbols, and numbers.

5. Never provide personal information to third parties and even to family and friends.

6. In case of contact with a bank or any company, a genuine company will never ask for personal information (except for a code word). Any genuine company always has all the information required to help its customer. In this case, it does not matter who initiated a phone call or an appointment.

4.5 Inferential Analysis

This subsection is intended to test all the hypotheses put forward during the descriptive analysis. The inferential analysis provided an opportunity to determine which hypothesis could be accepted and which one to reject. Hypothesis testing assisted to provide more reliable answers to the research questions and achieve the stated objectives.

As discussed in Chapter 3, Chi-square test was used to test the hypotheses. The researcher decided to use the Chi-square because this method includes its robustness with respect to distribution of the data, its ease of computation, the detailed information that can be derived from the test, its use in studies for which parametric assumptions cannot be met, and its flexibility in handling data from both two group and multiple group studies. The Chi-square test determined the p-value for the hypotheses being tested. After calculating the p-value for each hypothesis, the researcher compared the result with the significance level. The significance level is assumed to be 5% (0.05), which means
that the hypothesis has a confidence level of 95%. In other words, if the p-value is less than or equal to the significance level, then the researcher rejected the null hypothesis in favor of alternative hypothesis. However, if the p-value is more significant than the significance level, the researcher did not reject null hypotheses.

To prepare for each step of hypothesis testing, the researcher created a cross-tabulation of the variables that was used to test each hypothesis. All testable hypotheses the researcher designed were based on the research participant’s answers in the online questionnaire. The following subsections of Section 4.5 are divided into each testable hypothesis that the researcher has generated to provide more reliable answers to the research questions.

4.5.1 Hypothesis 1

Null Hypothesis 1: There is no difference between New Zealand banking services users with different levels of experience in the falling victim of banking fraud and scams (The ability of New Zealanders to avoid banking fraud and scams does not depend on their banking experience).

Alternative Hypothesis 1: There is a difference between New Zealand banking services users with different levels of experience in the falling victim of banking fraud and scams (The ability of New Zealanders to avoid banking fraud and scams depends on their banking experience).

Findings: Table 1 shows the result of the cross-tabulation analysis between banking services users' experience and victim of banking fraud and scams. When testing the hypothesis, the researcher obtained a p-value = 0.8, which means p> 0.05 and was not significant. Therefore, the New Zealand community’s ability to avoid banking fraud and scams does not depend on their banking experience. Thus, Null Hypothesis 1 was not rejected.

Table 1
Cross-tabulation of banking services users experience and do not fall into fraud

<table>
<thead>
<tr>
<th>Experience, years</th>
<th>Yes</th>
<th>No</th>
<th>I do not know</th>
<th>Total by experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3</td>
<td>6</td>
<td>21</td>
<td>2</td>
<td>29</td>
</tr>
<tr>
<td>4-6</td>
<td>7</td>
<td>19</td>
<td>1</td>
<td>27</td>
</tr>
<tr>
<td>7-10</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>10-15</td>
<td>2</td>
<td>14</td>
<td>0</td>
<td>16</td>
</tr>
<tr>
<td>more than 15</td>
<td>11</td>
<td>22</td>
<td>2</td>
<td>35</td>
</tr>
<tr>
<td>Total by victims</td>
<td>27</td>
<td>81</td>
<td>5</td>
<td>113</td>
</tr>
</tbody>
</table>

Expected values
### 4.5.2 Hypothesis 2

Null Hypothesis 2: Banking service users' knowledge of the types of fraud and scams does not depend on their experience of using banking services.

Alternative Hypothesis 2: Banking services users' knowledge of the types of fraud and scams depends on their experience of using banking services.

Findings: Table 2 shows the result of the cross-tabulation analysis between banking services users' knowledge about fraud and scams typology and their years of experience in banking services. When testing the hypothesis, the researcher received a p-value = 0.00006, which means p < 0.05, which was significant. Therefore, banking services users' knowledge of the types of fraud and scams depends on their years of experience of using banking services. Moreover, by looking at the descriptive analysis, the researcher noticed that every research participant of the online questionnaire mentioned at least four familiar types of banking fraud and scams. For this reason, Null Hypothesis 2 was rejected.

### Table 2

Cross-tabulation of banking services users' experience and knowledge of the types of fraud and scam

<table>
<thead>
<tr>
<th>Experience, years</th>
<th>Highly familiar, number</th>
<th>Not much familiar, number</th>
<th>Fairly familiar, number</th>
<th>Total by experience, number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3</td>
<td>1</td>
<td>14</td>
<td>14</td>
<td>29</td>
</tr>
<tr>
<td>4-6</td>
<td>4</td>
<td>3</td>
<td>19</td>
<td>26</td>
</tr>
<tr>
<td>7-10</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>10-15</td>
<td>4</td>
<td>3</td>
<td>9</td>
<td>16</td>
</tr>
<tr>
<td>more than 15</td>
<td>16</td>
<td>1</td>
<td>18</td>
<td>35</td>
</tr>
<tr>
<td>Total by familiarity</td>
<td>26</td>
<td>23</td>
<td>64</td>
<td>113</td>
</tr>
</tbody>
</table>

**Expected values**
### 4.5.3 Hypothesis 3

Null Hypothesis 3: The experience of using banking services does not give an understanding on how financial institutions can protect society from fraud.

Alternative Hypothesis 3: The experience of using banking services gives an understanding on how financial institutions can protect society from fraud.

Findings: Table 3 shows the result of the cross-tabulation analysis between banking services users’ experience and their knowledge about financial institutions’ actions against fraud. When testing the hypothesis, the researcher received a p-value = 0.43, which means p > 0.05 and was not significant. Therefore, the experience of using banking services does not give an understanding that financial institutions can protect society from fraud. Null Hypothesis 3 could not be rejected.

#### Table 3
Cross-tabulation of banking services users' experience and knowledge about financial institutions' actions against fraud

<table>
<thead>
<tr>
<th>Experience, years</th>
<th>Highly familiar</th>
<th>Not much familiar</th>
<th>Fairly familiar</th>
<th>Expected values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3</td>
<td>6.67</td>
<td>5.90</td>
<td>16.42</td>
<td></td>
</tr>
<tr>
<td>4-6</td>
<td>5.98</td>
<td>5.29</td>
<td>14.73</td>
<td></td>
</tr>
<tr>
<td>7-10</td>
<td>1.61</td>
<td>1.42</td>
<td>3.96</td>
<td></td>
</tr>
<tr>
<td>10-15</td>
<td>3.68</td>
<td>3.26</td>
<td>9.06</td>
<td></td>
</tr>
<tr>
<td>more than 15</td>
<td>8.05</td>
<td>7.12</td>
<td>19.82</td>
<td></td>
</tr>
<tr>
<td>P-value</td>
<td></td>
<td></td>
<td>0.000062489148</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Experience, years</th>
<th>Yes</th>
<th>No</th>
<th>I do not know</th>
<th>Total by experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3</td>
<td>11</td>
<td>5</td>
<td>13</td>
<td>29</td>
</tr>
<tr>
<td>4-6</td>
<td>19</td>
<td>3</td>
<td>6</td>
<td>28</td>
</tr>
<tr>
<td>7-10</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>10-15</td>
<td>10</td>
<td>2</td>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>more than 15</td>
<td>20</td>
<td>6</td>
<td>8</td>
<td>34</td>
</tr>
<tr>
<td>Total by people</td>
<td>62</td>
<td>17</td>
<td>34</td>
<td>113</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Experience, years</th>
<th>Yes</th>
<th>No</th>
<th>I do not know</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3</td>
<td>15.91</td>
<td>4.36</td>
<td>8.73</td>
</tr>
<tr>
<td>4-6</td>
<td>15.36</td>
<td>4.21</td>
<td>8.42</td>
</tr>
<tr>
<td>7-10</td>
<td>3.29</td>
<td>0.90</td>
<td>1.81</td>
</tr>
</tbody>
</table>
4.5.4 Hypothesis 4

Null Hypothesis 4: The experience of using banking services does not impact the level of understanding on the extent of measures that the New Zealand Government takes to mitigate the risk.

Alternative Hypothesis 4: The experience of using banking services impacts the level of understanding on the extent of measures that the New Zealand Government take to mitigate the risk.

Findings: Table 4 shows the result of the cross-tabulation analysis between banking services users' experience and their knowledge about the New Zealand Government involvement in mitigating the risk of fraud. When testing the hypothesis, the researcher received a p-value = 0.429, which means p > 0.05 and was not significant. The experience of using banking services does not have an impact on the level of understanding on the measures taken by the New Zealand Government to mitigate the risk of fraud or not doing enough. Moreover, looking back to descriptive analysis, the researcher noticed that only 10% (n = 4) of research participants indicated that they understood the involvement of the New Zealand Government in mitigating the risk of fraud. Financial industry professional experts had a similar view on the New Zealand Government's involvement in mitigating the risk of fraud. They noted that financial institutions need more help to strengthen the legislative framework, cybersecurity and expand collaboration and information sharing between all stakeholders. For this reason, Null Hypothesis 4 could not be rejected.

**Table 4**

Cross-tabulation of banking services users experience and knowledge about New Zealand government involvement

<table>
<thead>
<tr>
<th>Experience, years</th>
<th>Yes</th>
<th>No</th>
<th>I do not know</th>
<th>Total by experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3</td>
<td>5</td>
<td>6</td>
<td>18</td>
<td>29</td>
</tr>
<tr>
<td>4-6</td>
<td>6</td>
<td>9</td>
<td>13</td>
<td>28</td>
</tr>
<tr>
<td>7-10</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>10-15</td>
<td>1</td>
<td>4</td>
<td>11</td>
<td>16</td>
</tr>
<tr>
<td>more than 15</td>
<td>2</td>
<td>12</td>
<td>20</td>
<td>34</td>
</tr>
<tr>
<td>Total by people</td>
<td>14</td>
<td>34</td>
<td>65</td>
<td>113</td>
</tr>
<tr>
<td>Experience, years</td>
<td>Yes</td>
<td>No</td>
<td>I do not know</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>-----</td>
<td>----</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>1-3</td>
<td>3.59</td>
<td>8.73</td>
<td>16.68</td>
<td></td>
</tr>
<tr>
<td>4-6</td>
<td>3.47</td>
<td>8.42</td>
<td>16.11</td>
<td></td>
</tr>
<tr>
<td>7-10</td>
<td>0.74</td>
<td>1.81</td>
<td>3.45</td>
<td></td>
</tr>
<tr>
<td>10-15</td>
<td>1.98</td>
<td>4.81</td>
<td>9.20</td>
<td></td>
</tr>
<tr>
<td>more than 15</td>
<td>4.21</td>
<td>10.23</td>
<td>19.56</td>
<td></td>
</tr>
<tr>
<td>P-value</td>
<td></td>
<td></td>
<td>0.42978</td>
<td></td>
</tr>
</tbody>
</table>

**4.6 Chapter Summary**

Chapter 4 described descriptive and inferential analysis used, which assisted the researcher to understand the research findings and draw robust conclusions. Based on the results of the descriptive analysis, the researcher generated four null and alternative hypotheses. All hypotheses were tested using the Chi-Square test. The researcher rejected one null hypothesis and accepted the alternative.

An in-depth analysis of the data allowed the researcher to lay the fundamental basis for identifying gaps in the current literature and further discuss the results (refer to Chapter 5) and formulate a comprehensive answer to the three research questions aimed at reducing the risk of banking fraud and scams in New Zealand.

The research participants' understanding of the types of fraud prevalent in New Zealand and a comparison of these types of fraud and scams with the opinion of financial industry professional experts and the literature review provided a comprehensive answers to the first research question.

Banking services users provided feedback on the level of engagement of the financial sector and the New Zealand Government in mitigating the risk of fraud. At the same time, financial industry professional experts outlined the existing achievements for mitigating the risk of fraud and the current problems. The analysed data received from the banking service users and the financial industry professional experts, and world practitioners allowed concluding the level of involvement of Government and financial institutions mitigating the risk of fraud and provided recommendations for improving the situation.

The advice from financial industry professional expert advice banking services user’s insights assisted the researcher to create a simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud and scams.
CHAPTER V: FINDINGS AND CONCLUSION

5.1 Introduction

Chapter 5, discussed the results obtained from descriptive analysis and inferential analysis, which are presented in Chapter 4. In the first section of Chapter 5, the researcher reviews the information collected during the research and then compares the results obtained with the theoretical and industry basis discussed in Chapter 2. The researcher devotes the following section of Chapter 5 to a discussing the contribution of the research results, and sets out the consequences of scientific discoveries and concludes that the research objectives have been achieved. Finally, Chapter 5 concludes by identifying the limitations of this research and providing recommendations for future research based on the identified limitations and findings.

5.2 Overview of Findings

In Chapter 4, the researcher conducted a descriptive and inferential analysis for two groups of research participants - banking services users and financial industry professional experts.

The researcher received 113 responses from the banking services users’ research participants all based in New Zealand. Interaction with the online questionnaire research participants undertook was through LinkedIn, the professional social media platform. The researcher sent 283 invitations via LinkedIn. One hundred thirteen banking services users accepted the invitation and undertook the online questionnaire, which means the response rate to the invitation was approximately 40%. Seventy percent (n = 80) of the research participants provided answers to all the questions.

The researcher identified and invited five financial industry professional experts from the four most prominent New Zealand banks, covering more than 90% of the New Zealand banking sector to undertake a face-to-face interview. All the financial industry professional experts met the criteria given in Chapter 3. During the face-to-face interview, the researcher advised the research participants that they could skip any question if they did not want to answer it for any reason, with no explanation. However, all the financial industry professional experts provided answers to all questions without exception.

Based on the descriptive analysis and inferential analysis, the researcher was able to draw reliable conclusions and obtain answers to the three research questions identified in Chapter 1.

The researcher formulated four hypotheses, which, after cross-tabulation, assisted in obtaining more reliable answers and conclusions to the first and second research questions.
The adoption of Null Hypothesis 1 suggested that the critical factor in mitigating the risk of banking fraud and scams is not New Zealanders' experience of using banking services. Moreover, the adoption of null hypotheses 3 and 4 suggested that the experience of banking services users does not allow New Zealanders to understand how much the Government and financial institutions are involved in the process of combating banking fraud and scams and what measures they are taking.

The researcher found that the level of experience in using banking services affects the banking services users’ knowledge on the typology of banking fraud and scam which suggests acceptance of the second alternative hypothesis.

According to null hypothesis 1, the extent of banking services user’s experience is important in understanding the types of fraud. It means that for banking services users to mitigate the risk of banking fraud and scams, it is necessary to have a comprehensive understanding of the typology and know all possible types of scams. However, alternative hypothesis 2 shows that experience in banking is not important in avoiding fraud. Besides, banking services users need to follow essential safeguards to avoid any kind of banking fraud with a 93% probability (the remaining 7% occur without the involvement of banking services users' BIN attacks, see Chapter 2 and Chapter 4). The researcher presents a simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud and scams in the next section of Chapter 5.

5.3 Comparison of Research Findings and Theoretical Framework.

This section discusses the research results conducted using the face-to-face interview and the online questionnaire. The researcher compared the data obtained during the face-to-face interviews and the online questionnaires with the literature review of banking fraud and scams presented in Chapter 2. Among the research variables, "common forms of banking fraud and scams in New Zealand" and "New Zealand Government and financial institutions involved in combating fraud" produced results that enabled comparison with the theoretical framework presented in Chapter 2. Furthermore, following the findings in Chapter 2 and Chapter 4, the researcher developed a simple set of rules and guidelines for New Zealanders to avoid falling victim to banking fraud. Thus, in this section, the researcher answers the three research questions.
5.3.1 Common Types of Banking Fraud and Scams.

According to annual the Netsafe Report 2020, the most common types of banking fraud and scams are romance, investment, lottery, invoice, and phishing. To see the picture more clearly, these can be divided into two groups: in terms of the number of cases and of incurred losses. However, despite being grouped according to various criteria (the number of cases or the number of losses from the population), investment scams, romance scams, and phishing lead the identifying the three most common types of fraud and scams in New Zealand.

Based on the answers received during the research and their comparison with industry data, the researcher identified the three most common types of banking fraud and scams in New Zealand. Figure 31 and Figure 32 show a comparison of the most common types of banking fraud and scams in New Zealand. The researcher obtained data from three sources:

1. The official Netsafe annual report is generated based on the number of fraud cases reported by the New Zealand community through the Netsafe website (Netsafe 2021).

2. The researcher took data from the online questionnaire (banking services users), which was supposed to answer question about the known types of banking fraud and scams.

3. The researcher identified the three most common types of banking fraud and scams from financial industry professional experts based on their personal experience.

Figure 31
Comparison of the most common types of fraud in terms of cases
According to Figure 31 and Figure 32, the most common types of fraud in New Zealand are phishing, investment scam, and romance scam. Figure 31 and Figure 32 do not compare results between groups. The researcher obtained the percentage of data based on the following calculations: for bank service users and financial industry professional experts - the number of mentions of a particular type of fraud in the total number of research participants (face-to-face interviewees or online questionnaires). For instance, five financial industry professional experts out of five mentioned that romance scam and phishing were the most common types of fraud and scams. The data from the Netsafe Report was calculated based on the number of incidents or losses in the total number of incidents or losses, respectively (from Netsafe Report 2021).

Figure 31 shows that phishing received the highest response from banking services users (83% (n = 93)) and financial industry professional experts (100% (n = 5)). Moreover, the Netsafe Report (2021) data showed that phishing in New Zealand accounts for 73% of all known fraud and scam cases and outnumbers any other type of fraud by at least seven times. According to the Netsafe Report (2021) and the financial industry professional experts, investment scam is the second most common in registered fraud and scam cases (11%), and references from financial industry professional experts (80%). However, investment scam is less familiar for banking services users than romance scam or lottery scam. Moreover, in terms of losses, an investment scam outperforms any other type of fraud despite fewer cases. A romance scam is also one of the most common types of scams in New Zealand. All financial industry professional experts (100%) mentioned romance scams as the most common
type of scam. Furthermore, the romance scam is 28% of all losses and is second only to an investment scam in terms of the number of losses incurred.

However, it is worth noting that there are lottery scams and invoice scams among the common, but not mentioned by financial industry professional experts (due to the limitation of the question). According to the number of reported cases, lottery scams account for 8% of all claims and exceed romance scams by 1%. Lottery scams and invoice scams are familiar to 74% and 62% of banking services users, respectively.

To obtain more reliable conclusions about the most common types of fraud and scams, research participants in the online questionnaire described the kind of fraud or scams the fraudsters were trying to commit. Figure 33 shows the distribution of responses from research participants in the online questionnaire by type of fraud and scam in which they believe they were involved.

**Figure 33**

Types of fraud and scams attempted on banking services users

According to Figure 33, phishing was the most popular type of scam. Phishing was identified and described by 33% (n = 26) who were involved in fraudulent events. Not one research participant named BIN-attack, it was determined this was due to unknown terminology. However, based on the descriptions of the fraudulent events provided, the researcher was able to identify a BIN attack for 10% (n=8) of the research participants. Another type of fraud with bank cards - skimming was
determined by 5% (n = 5) of the research participants. The third most popular was the investment scam identified by 6% (n = 6) of the research participants. The researcher ruled out BIN-attack and skimming types of fraud due to the minimal opportunity for banking services users to influence or avoid this type of fraud. In both cases, the bank compensates for fraud and scam losses of customers.

Based on the literature review analysis, the face-to-face interviews, and the online questionnaire, the researcher established the reasons for the dominance of phishing, investment scams, and romance scams in New Zealand.

1. Phishing. In terms of ease of distribution and reaching the most significant number of potential victims, was the most effective, as scammers spread malicious emails or messages to tens of thousands of people at the click of a button. Phishing emails or messages always look like genuine information, and it is complicated for the average user to distinguish fraudulent emails from genuine ones. According to the financial industry professional experts, the latest phishing activities in New Zealand are associated with companies such as the New Zealand Transport Agency, New Zealand Post, and New Zealand IRD. For instance, thousands of New Zealanders have received a phishing email stating that their car registration is about to end and they need to pay a registration fee. In terms of information in an email, the only difference between fraudulent and genuine is that the genuine email contains personal data of the client and the car. In contrast, a phishing email cannot contain such data because it is sent to thousands of addresses simultaneously. Another example is from the New Zealand Post: thousands of people have received a message stating that a package is waiting for them, and they need to pay $1.50 NZD to deliver the package. Naturally, thousands of people in New Zealand use online shopping or are just waiting for parcels from their friends and relatives. A similar situation occurred with the New Zealand IRD when thousands of people receive a message that they are awaiting a refund of taxes paid, and to receive a refund, they must provide a bank card number. Moreover, other famous companies such as banks, medical institutions, and government agencies have been susceptible to phishing attacks.

2. Investment scam. The main reason for the prevalence and popularity of investment fraud is the desire of people to become rich quickly and without investing much time and expense. In this case, fraudsters do not have to find people with huge savings. The main trick is they offer to invest a small amount at the start, and the result will be an amount ten times higher than the invested one. Victims will then be shown some visually persuasive graphics while the fraudsters continue a dialogue for them for what may be weeks, months, or even years, all the while telling them how well the investment is performing (Salsabila, 2018). When the victim wants to withdraw the funds, the fraudsters advise that a withdrawal fee must be paid, thus siphoning more money from the victim. These fees will
steadily increase, and the victim will never see any actual monetary returns, while the fraudsters essentially can do what they like with the money. Victims will then try to recover their funds any way they can and usually defer to fake "scam recovery services," often run by the same fraudsters purporting the original investment scam.

3. Romance scam. The main reason for the prevalence of romance scams is people's loneliness and the desire to find a loved one and/or start a family. The victims of romance scams are the elderly, bereaved, or young people who are desperate to find a partner and start a family. The scammers also did not stop during the lockdown due to the COVID-19 outbreak. Scammers take advantage of lonely and bored people in isolation by posting fake profiles on social media and dating websites.

5.3.2 Government and Financial Institutions Response

According to the online questionnaire results, banking services users’ understanding of the involvement of the New Zealand Government and financial institutions in mitigating the risk of fraud in different ways. Figure 34 shows banking services users 'knowledge about the participation of the New Zealand Government and financial institutions in combating banking fraud and scams.

**Figure 34**

Financial institutions and the New Zealand government in combating banking fraud and scams

The research results show a significant difference between the efforts made by banks and the Government to mitigate the risk of fraud and scams. More than 53% (n = 61) say that banks are involved in mitigating the risks of fraud and can protect their banking services users. At the same
time, 12% (n = 14) of the research participants saw Government involvement in mitigating the risks of fraud. However, none of the 12% (n = 14) of research participants could provide what specific measures they see from the Government. Moreover, 25% (n = 28) of the online questionnaire research participants who noted the involvement of financial institutions (ticked “Yes”) in mitigating the risk of fraud and scams described specific measures by financial institutions. The minority of banking services users (12% (n=14)) were confident that financial institutions were not involved in mitigating the risk of fraud and could not protect their customers.

In contrast to this, more the 30% (n = 34) of research participants did not see the New Zealand Government's involvement in mitigating the risk of fraud. Furthermore, all (100% n = 5) financial industry professional experts noted that financial institutions and the New Zealand community lack Government support. However, Figure 35 shows that New Zealand's government and financial institutions need to strengthen their focus on community education, laws enforcement and punishing, stakeholder collaboration, and cybersecurity. Noting, that cybersecurity was not the subject of this research.

**Figure 35**
What measures the government and banks should take to mitigate the risk of banking fraud and scams

![Bar chart showing measures and number of answers](image)

5.3.2.1 Collaboration

According to Ahmed et al., (2014), the role of government agencies and financial institutes in mitigating banking fraud and scams cannot be overemphasised. Clementina & Isu (2016) invited
banks and governments to work together domestically and at the macro level to attract reputable foreign experts in fraud prevention, detection and security management to save any country from the hardships of increasing cases of banking fraud and insecurity. Another important aspect of fraud prevention is exchanging information and openness between industries, citizens, and government agencies. In this regard, the primary tool that allows citizens and companies to avoid fraud and scams is the availability of accurate, up-to-date online (Baz, et al., 2017).

Moreover, face-to-face interview research participants were convinced that exchanging information between financial institutions, the New Zealand Government, and other countries could effectively counter banking fraud. The financial industry professional experts advised establishing relationships between the Governments of New Zealand and India to crackdown on investment scams and phishing activities. According to financial industry professional experts' experience, most investment scams, phone scams, and phishing that target victims in New Zealand are run out of India.

One of the most effective fraud prevention measures is a collaboration between different financial institutions and payment services (Doeland, 2017). All banks are a closed system (Baz et al., 2017). Fraud in an isolated system and can only be detected in one system and not the entire banking industry (Doeland, 2017). Subsequently, fraud can spread like a virus and affect the whole system. However, with an advanced data exchange system between financial institutions, fraud would not extend to the entire system. In this case, an effective way to mitigate the risk of banking fraud establishing a significant information sharing process between banks and financial companies. The first step may be to create a single database accessible to all financial institutions. For instance, in Russia, the information-sharing process between banks has been operating since 2013 (Shulzhenko, & Romashkin, 2020). The information sharing process consists due to the fact that financial organisations detect fraudulent activity on the part of customers and enter information into a database indicating the personal data of fraudulent customers. All customers are checked through the database when opening accounts or providing other banking services. If customers find themselves in the database of fraudsters, the bank denies the customer access to any services and redirects the customer to the only State bank through which the customer can receive wages or benefits. Furthermore, the information in such a database can be beneficial for law enforcement agencies in conducting investigations and bringing perpetrators to justice.

However, banks alone cannot create such a database and create synergies within the industry and beyond. For this reason, the New Zealand Government must take the lead in fostering micro and macro interactions among all stakeholders in mitigating the risk of fraud.
5.3.2.2 Laws

An essential aspect in mitigating of risk of banking fraud and scams is a strict legislative framework, a system of punishment for fraudulent activity, and an understanding by potential fraudsters of the consequences in case of violation of laws.

Many scientific articles and studies suggest that law enforcement agencies have more problems than solutions in relation to fraud and scams (Yu hernawa, & Fakrulloh, 2021). The difficulties associated with accurately assessing financial losses from fraud and scams and the level of victimisation, fraud and scams pose many challenges for police regarding their ability to investigate, prosecute, or arrest fraudsters (Cross, & Blackshaw, 2015). Tracking and investigating in banking fraud and scams in connection with virtual and transnational elements of the crime is problematic for law enforcement agencies (Mason, & Bohm, 2017). Offenders use jurisdictional boundaries that prevent law enforcement from investigating and prosecuting (Yu hernawa & Fakrulloh, 2021). The above arguments look convincing and, indeed, are a serious obstacle on the way to catching fraudsters.

However, face-to-face interview research participants said that no natural law in New Zealand could criminalise those indirectly involved in fraudulent activities. According to financial industry professional experts, it is a known fact that fraudsters and scammers never transfer stolen money directly into their accounts. Fraudsters prefer to use so-called mules. They are a critical part of the banking fraud and scam ecosystem. Mules are people who receive money stolen from fraudsters and scammers into their accounts. After receiving money into their accounts, mules usually withdraw cash from an ATM. After that, they use companies to transfer money abroad (not banks) and the send money to fraudsters and scammers for a minimal fee. With this scheme, the ultimate recipient of the stolen money cannot be traced. This scheme does not work in New Zealand because all banks in New Zealand have an anti-fraud system capable of stopping or recalling international money transfers, but it is almost impossible to analyse and recall authorised transactions within the country since money withdrawals are instantaneous.

For this reason, the introduction of a law that would provide for the liability of mules is a key aspect in the mitigating of risk of all types of fraud and scams. The Police cannot arrest all fraudsters and scammers due to the cost and insufficient resources. However, the punishment would force other potential mules to think before acting. In addition, financial institutions always know the names of mules, which can also help bring them to justice for crimes. No one wants to receive a prison sentence for a symbolic reward or lose Government benefits.
Moreover, the New Zealand Government can oblige financial institutions to immediately close accounts and terminate relationships with customers who received the stolen funds. A mule without a bank account is not a mule and is useless for fraudsters. All the measures above would decrease the number of accomplices in fraud and scams, which would lead to a decrease in the number of fraudulent activities.

### 5.3.2.3 Education

Raising the financial literacy of all stakeholders and building trust in financial institutions is critical for the Government and financial institutions to prevent fraudulent activities in the financial market (Engels et al., 2020). In other words, it is better to say that one of the most effective measures to combat banking fraud and scams is the ongoing education of the New Zealand community and the creation of a system of awareness of current trends in the field of fraud.

Moreover, 24% (n = 27) of the research participants in the online questionnaire (50% of all proposed measures) and 100% (N = 5) of research participants in the face-to-face interview said that only continuing education for citizens from primary school to senior citizens would help mitigating the risk of fraud. For instance, the both groups of research participants proposed the following:

1. Extend a school programme and teach intermediate school pupils to detect fraud and avoid it.
2. Provide free meetings/get together for communities and teach people how to recognise financial fraud and scam, especially senior people.
3. New Zealanders of all ages and demographics need to be educated about a financial fraud and scams as it is as prevalent here as it is in other countries.
4. Use social media channels, and television and radio.

One of the critical points in this area is creating a coverage system of anti-fraud and scam activities in the media and via the Internet (Grohmann et al., 2018). This system would help increase literacy and recognition of fraud and scam types, reduce the tolerance for violations, and strengthen bona fide market participants (DeLiema et al., 2020). Several private companies in New Zealand (Netsafe, 2021) and the New Zealand Police have websites dedicated to banking fraud and scams. According to financial industry professional experts, these websites contain only basic information about fraud and scams but lack updates or trends. Although these websites are accessible to anyone, they are little known due to the Government and financial institutions' lack of good advertising campaigns in this regard. In addition, the primary victims of banking fraud and scams are the elderly,
many who are lacking in computer literacy around fraud and scams on the Internet and in relation to other modern technologies. For this reason, regular dissemination of information with real examples via radio and television could be an effective measure to increase the level of education and awareness of fraud and scams. For example, the Central Bank of Russia (2021) is recruiting the most popular television channels to participate in a financial literacy campaign featuring financial industry professional experts and citizens affected by fraud and scams.

According to three banking services users' responses, one of the effective measures to raise awareness among the New Zealand community about banking fraud and scams could be the distribution of advertising brochures by financial institutions; suggesting all financial institutions must distribute free brochures and flyers with educational materials on fraud and scams to their customers. Moreover, banks could disseminate information about fraud and scams through online-banking notifications and banking services users' emails. Even though this measure requires additional costs, it could lead to a decrease in the level of banking fraud and scams, and increase in banking services users’ loyalty and trust, and banks would save funds that they reimburse victims for in the case of financial losses.

The Government and financial institutions' awareness campaigns would aim to spread awareness of financial fraud and scams and underlying malpractice, including potential risks and remedies (Engels et al., 2020). Furthermore, information from the Government and financial institutions should help build an understanding of the responsibility and inevitability of punishment for fraud and scams among the New Zealand community. For instance, as part of the Saudi Arabian National Bank outreach campaign against fraud and scams, the Police and Federal Bank Officers travel to financial institutions, schools, and universities to build zero tolerance for banking fraud and scams among citizens (Baz et al., 2017).

5.3.3 Set of Rules to Avoid Fraud

Following global practice and research conducted among banking services users and financial industry professional experts, the researcher has compiled a short set of rules on how to mitigate the risk of banking fraud and scams for the New Zealand community:

1. Never provide sensitive information (bank card number, online banking credentials, IDs) over the phone, email, messages, or to strangers. Genuine people or companies will never ask about sensitive information.
2. Do not answer phone calls from unknown or unexpected (overseas) numbers. Block incoming phone calls from unknown numbers.

3. Make sure that a phone call is coming from a genuine company by asking them to send an email or mail confirmation as to what is happening. Double-check - find a genuine phone number of the calling company via open search on the Internet, make your call and clarify before action.

4. Regularly (fortnightly), change passwords from online banking, emails, or any accounts, and make different passwords for different accounts. Do not save passwords in the history of Internet browsers.

5. In case "it happened with me", spread your funds among different accounts and different banks.

6. Set up bank card transaction limits via a Banking App. For example, a daily limit or one transaction limit. It can help to avoid significant losses. Limits can be changed online before making a genuine transaction.

7. If you receive nameless or suspicious emails/text messages, do not click on links immediately delete received correspondence from the unknown and unexpected sources. A genuine email or will contain correct personal information. For example, a genuine New Zealand Transport Agency email will have the owner’s valid name and car information.

8. Before investing, do your research about a broker and collect feedback from the community and the Internet. The best option before investing money is checking the investment opportunity via the FMA website (https://www.fma.govt.nz/). This legitimate company belongs to the New Zealand Government and contains possible investment opportunities and a list of genuine and fraudulent providers.

9. In romantic relationships via social media or dating websites, never provide sensitive information or transfer money/gifts before meeting a person face-to-face and making sure the feelings are mutual.

10. When making purchases through social media networks or trading platforms (Facebook, Trade Me), make sure the seller is reliable, check the feedback, try to pay for the goods at the time of receiving.

11. Do not trust an advertisement with extremely cheap goods (televisions, vacuum cleaners, etc.). Too good to be the true.
5.4 Contribution

The results of this research are significant for different groups of people and companies and can be used to benefit the New Zealand community. For example, because this research described a wide range of banking fraud and scams and showed that phishing, investment and romance scams are the most common fraudulent activities, it becomes easier for all stakeholders to identify them. Now that there is an understanding of what types of banking fraud and scams are most common in New Zealand, and what methods and tricks are used by fraudsters and scammer to mislead potential victims, fraud and scams can be identified early and prevented.

New Zealanders, including the Māori, can use this research to educate themselves and raise personal and family awareness about the types of banking fraud and scams prevalent today and how to avoid becoming a victim of fraud and scams. Furthermore, New Zealanders can share research findings with their communities or over the Internet worldwide, thereby increasing awareness internationally. This research provided insight into what New Zealanders (banking services users and financial industry professional experts knew about how the Government and financial institutions were protecting them against fraud and scams and what steps might be taken in the future. Finally, this research could have laid the seed of intolerance for fraud and scams among people who are potential accomplices of fraudsters and scammers - mules.

Another group who could benefit from this research is the New Zealand Government and financial institutions; they could use the research results to analyse the effectiveness of actions taken to mitigate the risk of fraud in the past and design new mitigation strategies to counter banking fraud and scams in the future. Better practices from other countries, the opinions of financial industry professional experts, and insights from the New Zealand banking services users suggest that the Government and financial institutions can do much more to mitigate the risk of fraud and scams.

It is envisaged that this research will pave the way for future financial crime researchers and lead to discoveries to ensure the safety of citizens and companies to mitigate the risks of fraud and scams, globally.

Lastly, for future financial crime researchers, investigating the identification and prevention of banking fraud and scams both in New Zealand and globally the current research findings will provide information to support further bridging of the gap created by established industry practice and theoretical frameworks.
5.5 Implications and Conclusion

Whether the research findings were established in simple descriptive and inferential analysis (hypothesis testing), this research has vast practical applications. The research results indicate that it is vital for identifying and preventing banking fraud and scams for people, companies and Governments. Moreover, the researcher could not find analogues of this research within the financial industry and world practices.

This research confirmed that 100% of the online questionnaire undertaken by banking services user research participants were familiar with at least four types of banking fraud and scams. However, only 22% (n = 25) of banking services users believe that their level of understanding of fraud and scams is high. Null hypothesis testing has shown that banking services users' awareness of and types of banking fraud and scams does not depend on their experience of using banking services. The face-to-face interviews with financial industry professional experts also, suggests that banking services users and financial industry professional experts have a similar understanding of the types of fraud and scams that are prevalent today. An analysis of official sources of information on the number of cases and types of fraud and scams has confirmed the opinions of financial industry professional experts and bank services users that phishing, investment and romance scam are the most common in New Zealand.

The research also found that banking fraudsters and scammers attacked 50% of the banking services users. However, exactly half of the banking services users could avoid fraud and scams by using various methods or by identifying the fraud/scam at an early stage. According to the hypothesis tested, experience with banking services was an essential factor in avoiding fraud, suggesting that prevention does not require a deep understanding of the typology of fraud and scam (null hypothesis 1 versus null hypothesis 2) but only needs to follow basic precautions.

This research indicates that 70% of New Zealanders who were victims of fraud and scams have received support from their banks. This support included immediately blocking a compromised bank card or online banking, replaced a bank card or restored online banking access, and returned the stolen funds to customers. The listed measures above were the solutions to a fraud or scam that had already occurred and does not prevent or mitigate the risk of banking fraud and scams in any way. In addition, 54% (n = 61) of banking services user research participants that undertook the online questionnaire acknowledged the support of banks and are confident that banks can protect them from fraudulent encroachments. Eight one percent of clients of several banks report the identical quality of protection provided by banks. However, the picture is entirely different from the actual involvement
of the New Zealand Government in the mitigation of the risk of fraud and scams. The minority of research participants (12% (n = 14)) acknowledged the participation of the New Zealand Government in the mitigation of the risks of fraud and scams. The rest of the research participants of the online questionnaire did not provide support to indicate active mitigation of the risks of fraud and scams by the Government. Furthermore, the opinions of financial industry professional experts and banking services users regarding the participation of the Government in mitigation of risks of fraud and scams were highly similar. Both groups of research participants mentioned that it was necessary to develop education and awareness, collaborations, and change laws, which coincide with the best world practices.

In conclusion, this research provided answers to the three research questions identified. The most common types of banking fraud and scams were identified through banking services users undertaking an online questionnaire, some of whom were victims of fraud and scams, by face-to-face interviews with financial industry professional experts and comparing the opinions of the two groups with industry data. The involvement of the New Zealand Government and financial institutions in mitigating the risk of fraud scams was analysed based purely on personal opinions of banking services users, professional opinion of financial industry professional experts, and information found from official sources. Based on these insights, findings, expert opinion, and the world's best practices, the researcher proposed measures to strengthen mitigating the risks of fraud and scams and developed a set of rules to avoid fraud and scams.

5.6 Limitations

This research has several limitations due to the applied methodology and approach to the research. Due to the global COVID-19 pandemic, which limited the entry of additional potential research participants and limited the researcher's ability to invite more research participants due to negative environment and people’s mood related to the pandemic. Quarantine conditions and isolation also played a role in limiting the spread of the research to the other regions. For these reasons, the researcher identified research participants using the Internet (LinkedIn) and known colleagues of the researcher and their supervisor within the banking industry in New Zealand. The rest of the restrictions are shown below.

The first limitation is associated with choosing a professional social media network - LinkedIn. To select potential research participants, the researcher used the world's largest networking platform, LinkedIn. The problem was that most LinkedIn users are professionals in a particular industry and
may have a certain level of qualification, especially in banking or cybersecurity, which could affect the research results in understanding the types of fraud and scams and methods of struggle. The researcher did not analyse the research participants in relation to their level of education. Secondly, even though LinkedIn is the largest professional social network, it is significantly inferior regarding the number of users to other worldwide social networks. The use of social networks such as Facebook could have provided more research participants. Still, the researcher decided not to use such social networks because of the rules and restrictions within these networks.

The second limitation is related to the LinkedIn rules. To invite a potential research participant, the researcher had to make personal contact, which took from three to five days and limited the researcher in terms of time and number of research participants.

The third limitation was the language that the researcher used. The online questionnaire tool was available only in English. Moreover, communication with potential research participants, was limited by the researcher's knowledge of only Russian and English.

The fourth limitation stemmed from the fact that the research was focused only within New Zealand. Financial industry professional experts and banking services users were people who live in New Zealand. However, the researcher analysed the world literature and best practices in the field in mitigation of the risks of fraud and scams. Furthermore, the researcher found that extensive research on the topic of fraud and scams has been carried out globally over the past ten years, but the researcher was unable to find detailed analysis and research about the questions identified in this current research.

Although this research had several limitations due to the problematic situation in the world and New Zealand, research methods and approaches did not prevent the completion of the research. In addition, the limitations described above open prerequisites for future researchers.

5.7 Recommendations

Regardless this research achieved three of its objectives and answered the three research questions, the aggregate law could be used to further research the topic of banking fraud and scams. Outlined below is a list of possible ideas for additional research into the identification and prevention of fraud and scams.

First, the essential recommendation is to conduct research to address the limitations and gaps in the Section 5.6. For instance, to obtain more reliable answers to the research questions, it would be necessary to expand the sample of research participants including several dominant languages from
throughout the world (Mandarin, Hindi, Spanish, etc.) and comparing the results obtained in New Zealand with other countries.

Secondly, this research did not prioritise the technical aspects of banking fraud and cybersecurity. In this case, it would be helpful to research what technical methods (artificial intelligence, machine learning, etc.) are used by fraudsters and scammers to gain access to banking services users' personal information. In this case, research could be undertaken on how banking services users can reduce the risk of banking fraud and scams by adhering to technical regulations and security practices. What measures need to be taken by the Government and financial institutions to ensure cybersecurity.

Thirdly, additional research is required to identify current global trends in banking fraud and scams and what factors influence the emergence of new types and the disappearance of old ones. Understanding how services and products in the banking market motivate fraudsters to invent new types of fraud and scams would help prevent these before they emerge and spread to the public.

Fourthly, research is required to understand why the presence or absence of the banking experience among banking services users plays a role in reducing or increasing the risk of fraud and scams. Knowing the typology of fraud and scams, understanding how they work and is independent of experience.

Finally, this research allowed us to identify common types of fraud and scams and government agencies' involvement and develop a list of measures to mitigate the risk of fraud and scams. To understand the context underlying the research findings, further research is required that goes beyond objective perception and considers the subjective and psychological aspects of committing fraud and scams. For example, what drives fraudsters and what social measures are needed to reduce the risk of fraud and scams. Furthermore, understanding the feelings and emotions of all stakeholders could help to conduct a deeper analysis of all the issues covered and provide more reliable findings. Using additional qualitative (surveys, focus groups, case studies) and quantitative (advanced statistical analysis) methodologies could also contribute to obtaining more reliable results.
References:


http://www.ijam-web.org/article.asp?issn=2455-5568;year=2018;volume=4;issue=1;spage=60;epage=63;aulast=Kaur


https://www.infona.pl/resource/bwmeta1.element.ID-ec1cc738-65d5-4a04-823e-


LinkedIn website (2021). https://www.linkedin.com/jobs/


Netsafe New Zealand official website (2021).  
https://www.netsafe.org.nz/romance-scams/

New Zealand financial market authority (FMA) official website (2021).  
https://www.fma.govt.nz/investors/scams/


https://www.visa.co.nz/search.html?q=skimming

https://mpra.ub.uni-muenchen.de/97454/1/MPRA_paper_96807.pdf


https://oro.open.ac.uk/49591/17/49591ORO.pdf


https://osf.io/preprints/socarxiv/sy65n/download


https://dspace.uii.ac.id/bitstream/handle/123456789/8124/Thesis_Fidelia%20Salsabila_13312049%20pdf.pdf?sequence=1&isAllowed=y


http://repository.ubaya.ac.id/34658/1/Anton%20Hendrik_Tightening%20Loose%20in%20Eradicating%20Card%20Fraud_2018.pdf


Appendix 1 – Face-to-face interview

The aim of this research is to investigate banking fraud in New Zealand and create a simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud or scam. In addition, the research will help to understand technological aspects and forms of bank fraud and scams in New Zealand. Moreover, the research will examine NZ government’s and financial institutions’ response in the prevention and control of bank fraud including what has been done until now and what else could be done in future.

For the purpose of easy recall and accuracy, please base your responses on your most recent experience related with banking fraud and scam.

To keep the employer’s privacy and to not disclose any sensitive information, please DO NOT mention the following:

1. Any information related with your colleagues and customers.
2. Any information related with software what you and your colleagues use during working hours.
3. Any scripts and algorithms what is related with your employer.
4. Other information what can create an information breach or can be sensitive for the employer, customers or yourself.

QUESTIONS:

1. Based on your experience, what are the three most commonly used forms of banking fraud and scam in New Zealand (name and describe them)?

2. What technological tricks and methods are used by fraudsters to mislead the victim and commit a crime (New Zealand or worldwide)?

3. To what extent your company can protect its customers against fraud and scam?

4. How does your company cope with the evolving nature of the changes in the techniques used by fraudsters?
5. How can your company and the financial industry be involved to mitigate the risk of banking fraud in New Zealand?

6. How do you think the government is supporting the fight against fraud and scam?

7. What government measures can help financial companies and their customers prevent and avoid fraud?

8. How can New Zealanders prevent or avoid banking fraud and scam without government and financial institutions support?

9. What methods and technologies can you advise users of banking services to avoid fraud (share your experience and best practices)?

10. Do you want to add anything else related to banking fraud and scam?

End of face-to-face interview:

Thank you for participating in the interview. We appreciate you taking the time to respond. The research results will be available on April 2022. If you require a personal copy, please supply your email address here, or contact the researchers: babee1@student.op.ac.nz, or farhadm@op.ac.nz
Identification and prevention of banking fraud and scam in New Zealand

This questionnaire aims to investigate banking fraud in New Zealand and create a simple set of rules and guidelines for New Zealanders to avoid falling victim to modern banking fraud or scam. In addition, the study will help to understand technical aspects and forms of bank fraud and scams in New Zealand. Moreover, the research will examine the NZ government’s and financial institutions’ response in the prevention and control of bank fraud, including what has been done until now and what else could be done in the future.

For the purpose of easy recall and accuracy, please base your responses on your most recent experience related with banking fraud and scam.

1. How many years have you been using banking services in New Zealand?
   - 1-3
   - 4-6
   - 7-10
   - 10-15
   - more than 15

2. How do you rate your familiarity with different forms of the most common scam in New Zealand?
   - a) Highly familiar
   - b) Fairly familiar
   - c) Not much familiar

3. Which forms below of scams are you familiar with?
   - a) Romance - a confidence trick involving feigning romantic intentions towards a victim
   - b) Investment - a deceptive practice in the stock or commodities markets that induces investors to make p...
   - c) Skimming - an illegal practice used by identity thieves to capture credit card information from a cardho...
   - d) Identity theft - stealing a person’s personal information, including name, bank account number
   - e) Lottery scam – a work by asking you to pay some sort of fee in order to claim your prize or winnings fro...
   - f) Phishing - a type of social engineering where an attacker sends a fraudulent message designed to trick ...
   - g) Invoice scam – sending of fake invoices to a potential victim
   - h) Other
4. If you answered "Other" for question 3, please describe type scam you familiar with.

5. Has somebody attempted to commit banking fraud or scam on you?
   - [ ] a) Yes
   - [ ] b) No
   - [ ] c) I do not know

6. If you answered "Yes" on question 5 - Could you describe the actions that fraudsters attempted? If you answered "No" - go to the next question.

7. Have you ever been a victim of banking fraud?
   - [ ] a) Yes
   - [ ] b) No
   - [ ] c) I do not know

8. If you answered "Yes" on question 7 - Have you got any support from the bank or the government? If you answered "No" - go to the next question.

9. Do you think the bank that you use is able to protect you from fraud?
   - [ ] a) Yes
   - [ ] b) No
   - [ ] c) I do not know

10. If you are a user of more than one bank, do you have similar experience with them with respect to your fraud and scam? Please explain below if you have had different experiences.

11. Do you feel government support mitigates the risk of banking fraud and scam in New Zealand?
   - [ ] a) Yes
   - [ ] b) No
   - [ ] c) I do not know
12. What do you think, how governments and financial institutions can protect New Zealanders from banking fraud and scams (or opinion, experience from other countries)?

Развернутый ответ

---

Do you know or previously used to avoid falling victim to a banking fraud scam? Please, share your insights.

Развернутый ответ

---

Thank you for participating in the interview.

We appreciate you taking the time to respond.

The research results will be available on April 2022. If you require a personal copy, please supply your email address here, or contact the researchers: balbaei@student.op.ac.nz, or farhadm@op.ac.nz
Appendix 3 – Consent Form

Identification and Prevention of Banking Fraud and Scam in New Zealand

Consent Form

I have read the information sheet concerning this project and understand what it is about. All my questions have been answered to my satisfaction. I understand that I am free to request further information at any stage.

I know that:

- My participation in the project is entirely voluntary and I am free to refuse to answer any particular question
- I am free to stop participating at any time without reasons explanation
- I aware that the online questionnaire or the face-to-face interview may contain questions that may cause mental harm. If I feel uncomfortable with any question I stop participating at any stage
- I can choose to withdraw information provided without giving reasons and without any disadvantage
- I cannot withdraw any information I have supplied after the data has begun analysis on 1 June 2021.
- My data will be destroyed at the conclusion of the project but any raw data on which the results of the project depend will be retained in secure storage for five years after which it will be destroyed. If it is to be kept longer than five years, my permission will be sought.
- I will receive a copy of the research findings once the research is completed, which will be emailed to me in an address I nominate at the end of the survey.
- The results of the project may be published and/or used at a presentation in an academic conference but my anonymity/confidentiality will be preserved
- I can ask to receive a copy of the research findings even if I did not nominate an address at the end of the survey by emailing the researcher, Evgenii Babenkov, at babee1@student.op.ac.nz.

Additional information given or conditions agreed to

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

I agree to take part in this project under the conditions set out in the Information Sheet.

……………………………………………  (signature of participant)
……………………………………………  (full name of participant – please PRINT)
……………………………………………  (signature of researcher)
……………………………………………  (full name of researcher – please PRINT)
……………………………………………  (date)

This project has been reviewed and approved by OPREC
Confidentiality Agreement

**Title of Project:** Identification and prevention of banking fraud and scam in New Zealand

**Name of lead researcher:** Evgenii Babenkov

**Name of the Department:** Applied Management, Otago Polytechnic Auckland International Campus

**Role of the lead researcher.** My role in this project is to complete the research on time and make it useful for New Zealand society.

I am participating as a: (tick all that apply)

☑ Researcher ☐ Transcriber ☐ Administrator ☐ Marker ☐ Analyst

I agree that:

- I will carry out the tasks assigned to me in this project mindful of the confidential nature of the research.
- I will keep confidential all information provided to me and will not disclose it to any third party except people involved in this research project
- I will not make or retain any copies and/or records of the data other than what is required for the research.
- I will return all copies and/or records of the data to the researcher at completion of my involvement with the research.

__________________________________________________________________________  (Person’s name and signature)

Evgenii Babenkov  ___________________________________________________________  (Researcher name and signature)

__________________________________________________________________________  (Date)