https://doi.org/10.34074/rere.00304

Article

EXPLORING THE IMPACT OF CHATBOTS ON CUSTOMER SATISFACTION AND BUSINESS EFFICIENCY IN NEW ZEALAND'S FINANCIAL SERVICES INDUSTRY

Kashmira More and Indrapriya Kularatne

OTAGO POLYTECHNIC AUCKLAND INTERNATIONAL CAMPUS

ABSTRACT

The emergence of Artificial Intelligence has disrupted the conventional ways of dealing with customers. Artificial Intelligence-powered chatbots are one of the outputs of this technological disruption. Although the capabilities of a chatbot have been widely recognised, its adoption in financial service institutions has caused arguments over data protection. Customers tend to become comfortable with the human-like chatbot due to it being non-judgmental. The research method used was secondary qualitative research techniques based on literature reviews. The objective of this investigation is to evaluate the rise of chatbot adoption in customer services in the financial service institutions of New Zealand. The findings of the research indicate a rise in chatbot adoption has also led to data privacy issues in customer services. The research intended to objectively evaluate chatbots, to determine their merit at the expense of data protection and recommend solutions to address data privacy problems with chatbots.

Keywords: Artificial Intelligence, Financial Technology (FinTech), Chatbots, Data Privacy, General Data Protection Regulation, Personal Information.

INTRODUCTION

The efficiency and effectiveness of chatbots in business have offered unique customer service opportunities. Conversational agents driven by Artificial Intelligence (AI), such as chatbots, have revolutionised customer service, notably in financial service organisations throughout the world (Singh, 2022). Technological improvements are inescapable, and the financial service institutions will constantly strive to improve its customer service via innovation (Bairy & Rashmi, 2021). Natural Language Processing (NLP) technology built on machine learning has been widely employed in the creation of AI-powered chatbots (Bairy & Rashmi, 2021).

The objective of this research was to evaluate the rise of chatbot adoption in customer services in financial technology (FinTech) in New Zealand (NZ). This article is divided into four components, the first is the emergence of chatbots in FinTech services, notably in customer services in NZ. Second, it examines whether the advent of chatbots has positive or negative impacts on FinTech in NZ. Furthermore, the research focuses on chatbot-related challenges such as data protection and chatbots being sentient. Finally, the research critically analyses alternatives to the data privacy vulnerabilities associated with AI-powered chatbots and makes recommendations to address these issues.

METHODOLOGY

Exploratory qualitative research techniques based on secondary information were used to dig deep into the data and analyse responses, patterns, and connections. Secondary data was gathered from various online databases such as Google Scholar, Research Gate, Emerald Insights, Science Direct, ProQuest and SpringerLink. This method is cost-effective because all data used in this research was collected from published sources. No primary data was collected for this research. The collection of contemporary and relevant data is important for the validity of research based on secondary data (Asenahabi, 2019). The majority of the resources used in this research are not only current but were published in the last five years in peer-reviewed journals.

LITERATURE REVIEW

RISE OF CHATBOTS IN CUSTOMER SERVICE

In the early 60s while AI evolved, a chatbot named 'ELIZA' was introduced to conduct simple conversations with humans (Carter & Knol 2019; Paliwal et al., 2020). However, this technology has gained momentum in the past decade (Suta et al., 2020). For instance, the journey of chatbot evolution from ELIZA to Artificial Linguistic Internet Computer Entity (A.L.I.C.E) in 1995, Siri in 2010 and lastly ChatGPT in 2022 has been under the domain of AI, using NLP and Machine Learning Techniques (MLT) (Suta et al., 2020). In other words, chatbots have evolved from being able to respond to simple human conversations to complex human interactions which are currently contributing to enhancement in customer service (Murphy, 2023).

Chatbot is an application developed with the help of AI and machine learning techniques to interact with humans (Shawar & Atwell, 2007). For instance, Siri was developed by Apple, Alexa was developed by Amazon, Google Assistant and Chat GPT by Open AI (Shawar & Atwell, 2007). With the rise of AI via Machine Learning and Deep Learning Algorithms, chatbots have gained tremendous momentum in the service industries (Carter & Knol 2019; Sugumar & Chandra, 2021). Research evidence shows that AI has significantly altered the service industries by enhancing customer services and engagement (Carter & Knol 2019; Misischia et al., 2022; Sharma et al., 2022).

The service industries have been customer-facing since their inception (Misischia et al., 2022). However, the traditional customer-facing roles have been taken over by chatbots and have changed the theme of customer services over the past decade (Misischia et al., 2022). Conventionally, the role of customer services demands five vital functions namely interaction, problem-solving, customisation, trend, and entertainment (Misischia et al., 2022). Taking into consideration customer service in financial institutions, chatbots are used in the claim submissions process which provides room for claim managers to focus on more productive activities and minimise tedious tasks (Sugumar & Chandra, 2021). This leads to better customer service overall.

CHATBOT ADOPTION FOR FINTECH FIRMS IN NEW ZEALAND

Regarding the adoption of chatbots in customer services, studies have shown that it is highly influenced by a research model developed by the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) (Sugumar & Chandra, 2021). This model is called the Belief Desire and Intention (BDI) model (Sugumar & Chandra, 2021). The model explains that the adoption of chatbots not only depends on the beliefs of customers but also on the desire to interact with a non-human agent. For instance, chatbots in financial advisory firms have experienced a high preference for chatbots by customers to resolve financial queries if the chatbot is friendly and always ready to help (Sugumar & Chandra, 2021).

According to a report published by AI Forum New Zealand (2018), investments in AI-based chatbots will rise to 99.5% in financial accounting firms which could support not only customer services but also financial analytics and reporting. This research also sheds some light on the top five drivers of the adoption of AI in NZ which are managing big data, automation, fast decision-making, cost reduction and optimisation of processes (AI Forum New Zealand, 2023).

AI Forum New Zealand (2018) forecast the AI adoption capacity of various sectors in NZ and out of the sectors presented, financial service institutions showed an estimated adoption of 71%. This means most of the FinTech firms in NZ would potentially restructure to substitute customer services with AI (AI Forum New Zealand, 2018). These statistics are strongly supported by Kapsis (2020) who stated, unlike small and medium-sized FinTechs, large-size FinTechs were in support of AI-based customer services and regulators.

Even though a number of studies have been published on chatbot adoption in other service industries like tourism, healthcare and higher education, limited research has been published on chatbot adoption by FinTech (Alt et al., 2021). In this regard, it could be inferred that the finance service institutions has been a late adopter of this technology as compared to other service industries. The adoption of chatbots in the form of robo-advisors can be traced back to 2008 when a United States-based FinTech company Wealthfront and Betterment was established (Dietzmann et al., 2023). The popularity of chatbots strengthened significantly in the 2014 when the biggest FinTechs in the European market began adopting AI-based chatbot models as robo-advisors (Dietzmann et al., 2023).

New Zealand typically has small and medium size business enterprises in a plethora of sectors that include FinTech (Clutch, 2023). Apart from Deloitte, Pricewaterhouse Coopers International Limited (PwC) and Accenture, the rest are small and medium-sized business enterprises (Clutch, 2023). Although the adoption of chatbots depends on various factors such as the technological capabilities of the end users and competition in the market, it has been widely adopted by many firms in NZ (AI Forum New Zealand, 2023). Moreover, the Asia Pacific region which includes NZ has been facing digital disruption in the wealth management field. Private financial firms have been compelled to relook at their existing customer services approach and rebuild on a technological platform (Deloitte, 2023).

In support of the growing popularity of chatbots in FinTech, a detailed study by Jung et al. (2019) reported varied reasons for the rise in chatbot adoption. One of the notable reasons was a bare minimum investment in chatbots which is comparatively lower than an actual human advisor who charged 3% of the project cost. Another significant reason is the increased dependency on smart gadgets and ease of use. Chatbots on smartphones are easy to use and provide logical resolutions (Jung et al., 2019). Likewise, Misischia et al. (2022), stated that chatbots are becoming more popular in FinTech due to the targeted solutions offered to result in better decision-making for customers.

TECHNOLOGY ACCEPTANCE - CHATBOT ADOPTION BY CUSTOMERS

Chatbot adoption by customers in FinTech can be analysed in terms of the Technology Acceptance Model (TAM) (Lai, 2017). Although this model continued to evolve until the late 2000s, the original model developed by Davis (1985) critically evaluates the behavioural factor that influences customers' acceptance of technology. According to Davis (1985), a customer's propensity to accept technology is highly influenced by its 'Perceived Usefulness' and 'Perceived Ease of Use'.

Although various studies have been conducted in support of these behavioural indicators of usefulness and ease of use being vital factors for customers to adopt a technology, some contrasting studies provide non-supporting evidence (Alt et al., 2021). In contrast, the same study argues that ease of use has a limited effect on technology acceptance compared to usefulness (Alt et al., 2021). Despite these arguments, Chan and Leung (2021) have shown supporting evidence that customers' acceptance of chatbots is highly influenced by 'Ease of Use'.

As per the Deloitte report, Eggers et al. (2019), states the early adopters of AI-based technology of chatbots was the public sector. The private sector is now gradually adopting chatbot technology. Based on this, it could be inferred that the financial service institutions in the public sector has been an early adopter of chatbot technology (Eggers et al., 2019). The adoption of chatbots for customer services has risen to 31% (Accounts Recovery, 2022). FinTech is expecting a steep rise in chatbot usage by customers to 109 million users by 2025 (Accounts Recovery, 2022). While the chatbot adoption rate by customers in the financial service institutions was slower in the early 90s, there has been an increase in demand from millennials who have been raised in a digital age (Abe, 2016). Moreover, the Coronavirus disease (COVID-19) pandemic has accelerated the adoption (Abe, 2016).

A supporting study by Fernández (2019), states similar findings in the financial service institutions, where chatbot adoption has extended to verticals such as payments, capital markets, banking, investment management and insurance. One of the significant reasons for the adoption of chatbots is that they are non-judgemental and make zero errors (Le & Rajah, 2022). In the same vein, Misischia et al. (2022), states that chatbots are the preferred means of customer service due to their ability to show persistent empathy and kindness while dealing with customer queries. According to Debecker (2016), chatbots could potentially continue to grow because customers expect businesses to answer their questions 24/7. It has also been determined that 45.9% of customers agreed that they prefer text over email and phone while communicating with businesses. Oruganti (2020) justifies the adoption of chatbots in financial service institutions with various facts, one of which is the chatbots' ability to gather data about competitors from the customers. It specifies financial service institutions prefer chatbots as virtual assistants over a human for supporting queries related to a loan, policies, and accounts (Le & Rajah, 2022). Similarly, Bhatti (2019), supports the growth of chatbots in the financial service institutions due to the collection of feedback from customers. The same author reported that chatbot adoption is on the rise in nations like USA, UK, India, and Canada particularly in the financial service institutions. Based on this evidence, it could be inferred that NZ would also follow the path of these countries in the adoption of chatbots in NZ FinTechs (Bhatti, 2019). Although FinTechs in NZ are open to adopting chatbots, the acceptance of customers is questionable.

IS CHATBOT ADOPTION FOR FINTECH FIRMS IN NEW ZEALAND HELPING OR BACKFIRING?

Artificial Intelligence is gradually being adopted by the private sector in NZ and NZ customers, which means private financial service institutions should consider deploying AI-based chatbots to enhance their customer service experience (AI Forum New Zealand, 2023). For instance, NZ customers are already familiar with AI agents like 'Josie for Auckland Savings Bank (ASB)', 'Union Bank of Switzerland (UBS) for Southern Cross', 'Jamie for Australia and New Zealand (ANZ) Bank', 'Hiko for Mercury' and 'Koa for NZ Post' (Newman, 2022). The NZTech (2019) states, growing humanness in the conversations with virtual assistants could result in improved sales and greater customer loyalty. Virtual assistants in the NZ financial service institutions have progressed beyond fielding routine inquiries. For example, 'Jamie,' an ANZ Bank chatbot, was optimised to avoid robotic replies and was able to react to 60% of customer enquiries (NZTech, 2019). There is a large amount of support and advantages promoted by major financial institutions in favour of chatbot adoption (Ravi & Kamaruddin, 2017). Over 80% of worldwide financial service institutions consider chatbots quite useful since they serve to increase corporate efficiency; however, just 16% consider chatbots to be genuine risks (Ravi & Kamaruddin, 2017).

Kruse et al's. (2019) analysis supports potential cost savings and increased productivity utilising chatbots in FinTechs, drawing on a wide range of sources. They claim that chatbots have improved customer service and engagement to a greater level (Kruse et al. 2019). Weißensteiner (2018) discovered that chatbots could not only recognise customer expectations but also discern their opinions. With AI technology underlying chatbot development, FinTechs such as robo-advisors are gaining popularity (Lui & Lamb, 2018). Investment banking and wealth management verticals of financial advisory firms advocate having robo-advisors as trusted agents in place of a human advisor who often tends to be selfish

(Lui & Lamb, 2018). Moreover, managing wealth is a delicate issue for everyone; thus, chatting with robo-advisors reduces the unpleasantness of the conversation for customers because of the absence of self-interest (Lui & Lamb, 2018).

Global financial service institutions like Barclay, Honkong and Shangai Banking Corporation (HSBC), Santander Bank, Bank of America, Swedbank and Deutsche Bank have robo-advisors in the form of chatbots and strongly believe chatbots have been offering their customers easy, economical, and non-judgemental financial advice (Lui & Lamb, 2018). However, they raised questions about the ability of robo-advisors in complex verticals of tax planning which could lead to severe losses to the FinTechs. Although there are mixed opinions on this, International Business Machines (IBM) Watson has preferred an approach of not disclosing to the customers whether they are conversing with a human or a chatbot. To overcome the fear of customers chatting with a non-human agent, IBM Watson has adopted 'Augmented Intelligence' in place of 'Artificial Intelligence' where humans train the chatbots. For instance, humans store the answers to the various scenario-based questions of customers in an electronic library, then Chatbots search the library to respond to customer queries and if they cannot find the answers, they refer the customers to human agents. In this manner, IBM Watson has overcome the issue of human versus chatbot and is able to provide flawless customer service. Inspired by IBM, several other FinTechs such as MortgageGym and Habito have executed a blend of chatbots and human advisors for complex wealth management verticals (Lui & Lamb, 2018).

In the past decade, there has been rapid development in integrating customer service via chatbots in FinTechs. Artificial Intelligence-inspired chatbots have gone beyond round-the-clock customer support and have helped FinTechs in improving compliance and regulatory requirements with 'Know Your Customer' (KYC) and 'Anti-Money Laundering' (A3Logics, 2023). A few success stories of AI-inspired chatbots in FinTechs are as follows: the Bank of America released their AI-inspired chatbot Erica in 2016, and it has since become very popular with customers on their mobile app and offers 24/7 service. Erica supports customers by providing financial advice and managing their accounts. It has inspired several other FinTechs to invest in chatbots and reap the benefits of cost savings and enhanced customer service. Unlike Erica, Capital One's Eno is an NLP-based chatbot that gives a real-time service to the customers of Capital One. Eno, unlike Erica, provides help via text messaging and communicates with customers via User Interface (UI) technologies. Eno has contributed to a significant reduction in operating costs, allowing the Capital One team to focus on strategic projects (A3Logics, 2023). It could be inferred that chatbots have been beneficial in the FinTechs not only in NZ but also globally.

While the use of chatbots in FinTech supports achieving a competitive edge and substantial cost savings in the long term, most FinTechs would not want chatbots to take over discussions about claims for a customer's death (Lui & Lamb, 2018). This is a highly sensitive issue, and financial service institutions cannot afford to bypass an in-person approach in such instances; nonetheless, this requires distinct research (Lui & Lamb, 2018). However, other authors have speculated that the rise of chatbots, particularly in FinTech, has also given rise to concerns related to data privacy (Alt et al., 2021; Sugumar & Chandra 2021). Moreover, contemporary arguments against chatbots include the fact that they are sentient (Tiku, 2022). Although, opponents now warn that if AI-based chatbots are given the same access and rights to make decisions as humans, computers may become more powerful than humans (Sugumar & Chandra 2021).

DATA PRIVACY ISSUES WITH CHATBOTS

Apart from chatbots being racist, biased, and manipulative, the problem of data privacy with chatbots is a source of discomfort for customers when interacting with them (Chaves & Gerosa, 2021; Lui & Lamb, 2018). For instance, Microsoft (MS) Twitter's chatbot named 'Tay' turned out to be making racial and offensive remarks within a couple of hours of its inception, which raised serious concerns about the morality of using chatbots (Chaves & Gerosa, 2021). Lui and Lamb (2018), have raised an interesting argument on the bias which could occur during the unsupervised training phase wherein the developer has the liberty to feed data that could be biased from a developer's perspective. Therefore, the main source of concern has been the rigid design of chatbots, which mostly lacks mechanisms to avoid data breaches (Calvaresi et al., 2021). Moreover, non-traditional data entry methods for chatbots may result in false resolutions and data privacy concerns for customers (Lui & Lamb, 2018).

On the other hand, customers regard chatbots as more intimate, which leads to stronger ties and the exchange of Personal Information (PI) (Le & Rajah, 2022). This relates to the adoption model and chatbots' lack of judgement, which makes customers more comfortable with communicating their concerns (Le & Rajah, 2022). The same authors have highlighted concerns regarding data privacy while using chatbots. Customers, on the other hand, choose to provide PI because they like interacting with chatbots. The data could be compromised with the simplest of security breaches such as unencrypted chats, failure to use Hypertext Transfer Protocol Secure (HTTPS) protocol and absence of Intrusion Detection and Prevention Systems (IDPS) (Sajan, 2022). Data privacy issues with chatbots are not only confined to sharing PI but also to storing and accessing data (Garkel, 2023; Pearce, 2021).

One of the data privacy concerns which could shift the ground beneath our feet is the privacy policy of the companies which develop AI-based chatbots. Chatbots collect PI from customers as a part of their job (Ferraro, 2023). However, customers have no choice on how this information is used or distributed once they share it with chatbots (Ferraro, 2023). For instance, the privacy policy of Chat Generative Pre-Trained Transformer (ChatGPT) developed by Open AI states that it gathers a customer's IP address, browser type, and preferences, as well as data about the customer's interactions with the site and surfing behaviours over time and across websites, which it may share 'with third parties without customer's consent (Open AI, 2023).

If customers refuse to share the required PI, the chatbot goes out of service (Ferraro, 2023). Moreover, if customers share PI and later want to delete it, there is no such option to remove it (Ferraro, 2023). These data privacy breaches often result in targeted advertising which customers may not be comfortable with (Garkel, 2023). The data privacy breach due to AI-powered chatbots could potentially result in cyber threats (Ferraro, 2023; NZ Herald, 2023). For instance, chatbots are designed to conduct a fluent conversation and replicate human emotions convincingly which could provoke attackers to recreate phishing emails or texts and initiate a malicious attack via fake advertising leading to identity theft and ransomware attacks (Ferraro, 2023; NZ Herald, 2023). In other words, cyber attackers may utilise chatbots to execute cyber-attacks using the PI kept by chatbots (NZ Herald, 2023). According to an article published in the New Zealand Herald (2023), cyber thieves may use chatbots such as ChatGPT to mimic financial service institution chatbots and obtain access to customers' PI.

Data privacy issues with chatbots are a growing concern and to combat the privacy risk, an ethical guideline for trustworthy AI set-up has been implemented. The General Data Protection Regulation (GDPR) which came into force in May 2018 is a significant initiative by the European Commission (Kapsis, 2020). The GDPR ensures provisions for data privacy related to transfer and process in relation to AI-powered technological developments (Kapsis, 2020). 'The Right to Erasure' (refer to articles 17 &19 of GDPR) establishes the right of customers to be excluded from search engine data; in other words, the right to withdraw consent from processing any PI collected by AI-based technologies that includes chatbots (Data Protection Commission, 2023). Sadly, simply enacting GDPR is not enough to address data privacy issues. According to an assistant professor at the University of Colorado, USA GDPR may obstruct future technological innovation (Greengard, 2018). Nevertheless, approaches to address chatbot data privacy issues will be considered in a later section.

ARE CHATBOTS SENTIENT?

Serious concerns have been raised about AI-powered chatbots being sentient, which means they can feel emotions and pain just like humans do (Almanzar et al., 2022). A group of authors with their research and testing have drawn attention towards making chatbots sentient with machine learning algorithms using different NLP modules (Tellols, 2020). Their research indicates that chatbots could be developed that are as sentient as humans and be more engaging for customers while conversing (Tellols, 2020). In contrast, Paul (2023) argues, chatbots at present are not sentient but statistical learning machines without an inner experience or a personality like a human. It is, after all, the humans behind these machines who modify the models and systems to make them work (Paul, 2023). In support of this argument, Eliabayev (2022) explains that chatbots are not yet artificially conscious and strongly advocates chatbots based on statistical models which are exposed to massive data creates the illusion of being sentient every time it provides responses which are intelligent.

Williams (2022) supports this view, claiming Google chatbot LaMDA has not passed the Turing Test and may not be called sentient. Therefore, it is hard to claim chatbots are conscious. On the contrary, chatbots are designed from language models to analyse words produced by humans online and generate language patterns in the form of responses. The theories about chatbots being sentient would intensify if debates about this topic were published more often, resulting in the creation of a large amount of data about AI becoming sentient. The more material there is about this topic, the more content AI chatbots will produce about it (Williams, 2022).

CRITICAL EVALUATION OF SOLUTIONS

Financial service institutions and FinTechs are among the world's most vulnerable to data security breaches (Whitman & Mattord, 2021). Financial service institution system cyber-attacks have recently flourished and are now ubiquitous (Doerr et al., 2022). A lack of authentication processes and poor authorisation has resulted in data breaches for FinTech in NZ (Ahmad et al., 2010).

The GDPR 2018 lays down extensive obligations for companies to become GDPR compliant. This means introducing AI-powered chatbots, whether in-house or via a third party, need to be GDPR compliant to protect the PI of their customers (Lishchynska, 2022). However, there is an argument as to what extent GDPR protects the data privacy of customers. For instance, AI-powered chatbots like ChatGPT and MS's Bing Chat, developed simply as a language model, may delete data without the customer's consent if the data is deemed to be not relevant (Stewart, 2023). This contradicts the GDPR of the 'Right to be Forgotten' (Stewart, 2023). As a result, being GDPR compliant is not enough to have chatbots protect the personal data of the customers (Stewart, 2023).

One of the greatest data privacy breaches in FinTech while using chatbots could be identity theft. This is when customer's data is leaked, and someone is impersonating or pretending to be the customer by using their PI (Te Tari Taiwhenua Internal Affairs, 2021). Chatbots are connected to the internet and customers tend to share PI such as credit card numbers, and bank account numbers to these chatbots to process their queries. If this information is not secured with a chatbot, it creates opportunities for hackers to steal PI in the absence of security measures such as firewalls, multifactor authentication and zero trust framework (Garkel, 2023). A survey conducted by Norton (2022) on identity theft in FinTechs in NZ states that 21% of New Zealanders have experienced financial identity theft (Gorrie, 2022). Moreover, this identity theft has risen by 86% since 2020 in NZ (Chiang, 2022). Identity theft in NZ as recent as 2020 with NZ-based FinTech Latitude Financial facing a severe identity theft wherein more than 97% of its personal data was compromised (Mcilraith, 2023). According to a leading NZ-based IT software services company, one of the major reasons for security threats with chatbots has been poor coding practices, lack of encryptions, and absence of security layers (Venugopal, 2023).

Nonetheless, these data security breaches could have been avoided with cyber security mechanisms for chatbots (Shalimov, 2022). The NZ-based FinTechs should adopt security mechanisms implemented by other global FinTechs to make chatbots cyber secure for customers. For instance, the chatbot used by Capital One banking 'Eno' is designed with anomaly detection to identify suspicious transactions, creates a virtual card number for each customer to protect them from identity theft (Shalimov, 2022). Another significant example of secured chatbots was launched by a US based company 'AlgoBot', being an intelligent chatbot used to monitor network securities and firewall administration (Barker, 2018). 'AlgoBot' is designed to monitor network traffic between Internet Protocol (IP) addresses, analyse connectivity problems between networks, identify a secure IP address, determine which application is affected due to security threats, and manage server traffic (Barker, 2018). Global FinTechs like American Express have machine learning fraud detection systems in place to detect anomalies (Mixson, 2021). Based on these security measures, it could be inferred that American Express have multi-layered security for its chatbot (Mixson, 2021).

RECOMMENDATIONS AND CONCLUSIONS

FinTechs in NZ could implement chatbots with security layers to protect customers' data privacy with multiple cybersecurity solutions. The first solution is 'Voice Biometric Technology' which can detect malicious voices of hackers across the networks (Pickup, 2022). In other words, 'User Behavioral Analytics' is an alternative which is developed with statistical algorithms to identify abnormal activities with conversational agents such as chatbots (Argus TrueID, 2023; Chotia, 2022). The second solution is 'End-to-End Encryption' of the conversations for customers which is also a responsibility under the GDPR (Preveil, 2022). Like WhatsApp chats, which are encrypted, FinTechs in NZ might adopt 'Public Key Encryption with Keyword Search (PEKS)' which enables customers to exchange information in an encrypted way but allows only the private key holder on the server end to decrypt the information (Biswas, 2020). Moreover, the third solution could be 'Two-Factor Authentication' which is a preventive measure for data leaks while conversing with chatbots (Chotia, 2022). Additionally, the fourth solution would comply with the GDPR of 'Self Destructing Messages' whereby FinTechs in NZ could implement a feature for customers to delete the messages after the chatbot session is over. The last solution could be a 'Web Application Firewall (WAF)' to stop any malicious code from being inserted into the customer's chatbot network from an intruder (Sajan, 2022). Chatbots based on the internet are vulnerable to malicious attacks (Fortinet, 2023). To prevent these threats and compromise customers' personal data security, WAF could act as an additional layer of security above network firewalls that are implemented to protect against unauthorised access (Fortinet, 2023).

Many FinTechs in NZ including banks like ANZ, ASB and BNZ have been using 128-bit Data Encryption Standard (DES) key encryption which is a security measure to protect against information leaks (Mills, 1997). However, there is no evidence of other security measures implemented to resolve data privacy issues. The main reason for not disclosing the chatbot design data protection mechanisms could also be to protect customer information from hackers. On the basis of the solutions recommended in the above, the researchers insist FinTechs in NZ implement a blend of all these solutions. For instance, although the network via which chatbots will have conversations with customers is encrypted, a WAF would provide protection from any malicious code being inserted into the customer's chatbot network (Fortinet, 2023; Sajan, 2022).

Moreover, Khan (2017) has recommended a blend of security measures to ensure adherence to data privacy for chatbots. For example, other than encryption and WAF, 'Self Destructing Messages' and 'Two-Factor Authentication' could be added as additional layers of security to protect the customer's personal data in chatbots (Khan 2017; Shaqiri, 2021). Lastly, 'Voice Biometric Technology' could represent a final layer of high-level security for chatbots. Implementing this technology itself could reduce multi-authorisation for customers (Argus TrueID, 2023; Raj, 2021). Chatbots are at the lead of innovation and therefore, FinTechs should invest in securing these conversational agents to protect data for their brand image as well as their customers' privacy.

REFERENCES

1 A3Logics. (2023). *How AI Chatbots Are Disrupting the Fintech Industry?* https://www.a3logics.com/blog/how-ai-chatbots-disrupting-fintech-industry

2 Abe. (2016). *How Financial Chatbots Are Transforming Digital Banking.* https://www.abe.ai/wp-content/uploads/2016/11/How-Financial-Chatbots-Are-Transforming-Digital-Banking-White-Paper.pdf Jung, D., Glaser, F., & Köpplin, W. (2019). Robo-advisory: opportunities and risks for the future of financial advisory. *Advances in Consulting Research: Recent Findings and Practical Cases*, 405-427. https://www.researchgate.net/publication/328390383_Robo-Advisory_Opportunities_and_Risks_for_the_Future_of_Financial_Advisory_Recent_Findings_and_Practical_Cases

3 Accounts Recovery. (2022, June 27). Chatbot Usage Growing in Financial Services. https://www.accountsrecovery.net/2022/06/27/chatbot-usage-growing-in-financial-services/

4 Ahmad, M. K. A., Rosalim, R. V., Beng, L. Y., & Fun, T. S. (2010). Security issues on banking systems. *International Journal of Computer Science and Information Technologies, 1*(4), 268-272. https://tinyurl.com/4kdw7vu4

5 AI Forum New Zealand. (2018). Artificial Intelligence. *Shaping a Future New Zealand*. https://www.mbie.govt.nz/dmsdocument/5754-artificial-intelligence-shaping-a-future-new-zealand-pdf

6 AI Forum New Zealand. (2023). *Towards our intelligent future*, https://aiforum.org.nz/wp-content/uploads/2019/09/Towards-our-Intelligent-Future_v1.01.pdf

7 Almanzar, A. D. Antic, A., & Taiuru, K. (2022). Can an AI be sentient?

8 Alt, M. A., Vizeli, I., & Săplăcan, Z. (2021). Banking with a Chatbot–A Study on Technology Acceptance. *Studia Universitatis Babes-Bolyai Oeconomica, 66*(1), 13-35. https://sciendo.com/article/10.2478/subboec-2021-0002

9 Argus TrueID, (2023). https://www.argustrueid.com/voice-identification/

10 Asenahabi, B. M. (2019). Basics of research design: A guide to selecting appropriate research design. *International Journal of Contemporary Applied Researches, 6*(5), 76-89.

11 Bairy, S.R., & Rashmi, R. (2021). A Review of Chatbots in the Banking Sector. *International Journal of Engineering Research & Technology (IJERT), 10*(6), 428-430. https://www.ijert.org/research/a-review-of-chatbots-in-the-banking-sector-IJERTV10IS060203.pdf

12 Barker, S. (2018). A chatbot for network security management? It's a reality. Security brief New Zealand. https://securitybrief.co.nz/story/chatbot-network-security-management-its-reality

13 Bhatti, A. (2019). Exploring the adoption of Artificial Intelligence in the Finance Industry: The case of Chatbots in the Kenyan Finance Industry. *Exploring the adoption of Artificial Intelligence in the Finance Industry: The case of Chatbots in the Kenyan Finance Industry (May 28, 2019)*. https://www.researchgate.net/profile/Athar-Bhatti/publication/338504388_Exploring_the_adoption_of_Artificial_Intelligence_in_the_Finance_Industry_The_case_of_Chatbots_in_the_Kenyan_Finance_Industry/links/607d9e378ea909241e1038ff/Exploring-the-adoption-of-Artificial-Intelligence-in-the-Finance-Industry-The-case-of-Chatbots-in-the-Kenyan-Finance-Industry.pdf

14 Biswas, D. (2020). Privacy Risks of Chatbot Conversations. Towards Data Science. https://towardsdatascience.com/hidden-privacy-risks-of-chatbot-conversations-881dbeeb98a

15 Calvaresi, D., Calbimonte, J. P., Siboni, E., Eggenschwiler, S., Manzo, G., Hilfiker, R., & Schumacher, M. (2021). EREBOTS: Privacy-compliant agent-based platform for multi-scenario personalized health-assistant chatbots. *Electronics, 10*(6), 666. https://www.mdpi.com/2079-9292/10/6/666

16 Carter, E., & Knol, C. (2019). Chatbots—an organisation's friend or foe? *Research in Hospitality Management, 9*(2), 113-116. https://www.tandfonline.com/doi/abs/10.1080/22243534.2019.1689700

17 Chan, W. T. Y., & Leung, C. H. (2021). Mind the gap: Discrepancy between customer expectation and perception on commercial chatbots usage. *Asian Journal of Empirical Research, 11*(1), 1-10. https://archive.aessweb.com/index.php/5004/article/view/4325

18 Chaves, A. P., & Gerosa, M. A. (2021). How should my chatbot interact? A survey on social characteristics in human–chatbot interaction design. *International Journal of Human–Computer Interaction, 37*(8), 729-758. https://arxiv.org/pdf/1904.02743.pdf

19 Chiang, J. (2022). Online identity theft is rising in NZ - here's what to do about it. eCommerce News New Zealand. https://ecommercenews.co.nz/story/online-identity-theft-is-rising-in-nz-here-s-what-to-do-about-it

20 Chotia, R. (2022). Conversational Chatbot Security: Threats, Measures, Best Practices. *Verloop.io*. https://verloop.io/blog/conversational-ai-chatbot-security/

21 Clutch. (2023). *Top Financial Services Firms in Auckland*, https://clutch.co/nz/financial-services/auckland

22 Data Protection Commission. (2023). *The right to erasure (Articles 17 & 19 of the GDPR)*. https://www.dataprotection.ie/en/individuals/know-your-rights/right-erasure-articles-17-19-gdpr

23 Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation, Massachusetts Institute of Technology). https://scholar.google.com/scholar?hl=en&as_sdt=0,5&q=Davis,+F.D.+(1986).+A+technology+acceptance+model+for+empirically+testing+new+end-user+information+systems:+Theory+and+results.+Massachusetts,+United+States:+Sloan+School+of+Management,+Massachusetts+Institute+of+Technology.&btnG

24 Debecker, A. (2016). *3 stats that show chatbots are here to stay*. Venturebeat. https://venturebeat.com/business/3-stats-that-show-chatbots-are-here-to-stay/

25 Deloitte. (2023). *Robot are here*, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sea-fsi-robo-advisers-asia-pacific.pdf

26 Dietzmann, C., Jaeggi, T., & Alt, R. (2023). Implications of AI-based robo-advisory for private banking investment advisory. *Journal of Electronic Business & Digital Economics*, (ahead-of-print). https://www.emerald.com/insight/content/doi/10.1108/JEBDE-09-2022-0037/full/pdf?title=implications-of-ai-based-robo-advisory-for-private-banking-investment-advisory

27 Doerr, S., Gambacorta, L., Leach, T., Legros, B., & Whyte, D. (2022). Cyber risk in central banking. https://www.bis.org/publ/work1039.pdf

28 Eggers et al. (2019). Quantum computing for finance: State-of-the-art and future prospects. *IEEE Transactions on Quantum Engineering, 1*, 1-24. https://ieeexplore.ieee.org/abstract/document/9222275

29 Eliabayev, U. (2022). Is Google's Chatbot Sentient? No, and Here's Why. *Haaretz*. https://www.haaretz.com/israel-news/tech-news/2022-07-03/ty-article/.premium/is-googles-chatbot-sentient-no-and-heres-why/00000181-c3e4-dcfd-a797-dbee545a0000

30 Fernández, A. (2019). Artificial intelligence in financial services. *Banco de Espana Article, 3*, 19. http://dx.doi.org/10.2139/ssrn.3366846

31 Ferraro, M. (2023). *Ten Legal and Business Risks of Chatbots and Generative AI*. Tech Policy Press. https://techpolicy.press/ten-legal-and-business-risks-of-chatbots-and-generative-ai/

32 Fortinet. (2023). *WAF vs. Firewall: Web Application & Network Firewalls*, https://www.fortinet.com/resources/cyberglossary/waf-vs-firewall

33 Garkel, A. (2023). *Privacy concerns over AI-based chatbots*. ETCisco.in. https://ciso.economictimes.indiatimes.com/news/privacy-concerns-over-ai-based-chatbots/97432534

34 Gorrie, M. (2022). The most common types of identity theft and top ten ways to avoid it. *Security Brief*. https://securitybrief.asia/story/the-most-common-types-of-identity-theft-and-top-ten-ways-to-avoid-it

35 Greengard, S. (2018). Weighing the impact of GDPR. *Communications of the ACM, 61*(11), 16-18. https://dl-acm-org.op.idm.oclc.org/doi/pdf/10.1145/3276744

36 Jung, D., Glaser, F., & Köpplin, W. (2019). Robo-advisory: opportunities and risks for the future of financial advisory. Advances in Consulting Research: Recent Findings and Practical Cases, 405-427. https://www.researchgate.net/publication/328390383_Robo-Advisory_Opportunities_and_Risks_for_the_Future_of_Financial_Advisory_Recent_Findings_and_Practical_Cases

37 Kapsis, I. (2020). Artificial intelligence in financial services: systemic implications and regulatory responses. https://www.proquest.com/docview/2524410664?parentSessionId=hsgWb2sIf09QjEGATqi66jnt4G1xXDhgO%2BOCvDcN61I%3D&pq-origsite=primo&accountid=39660

38 Khan, R. (2017). Standardized architecture for conversational agents aka chatbots. *International Journal of Computer Trends and Technology, 5*0(2), 114-121. https://www.researchgate.net/publication/321637578_Standardized_Architecture_for_Conversational_Agents_aka_ChatBots

39 Kruse, L., Wunderlich, N., & Beck, R. (2019). Artificial intelligence for the financial services industry: What challenges organizations to succeed. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/53b933fa-4961-48ca-bd6b-3ee8009edff9/content

40 Lai, P. C. (2017). The literature review of technology adoption models and theories for the novelty technology. *JISTEM-Journal of Information Systems and Technology Management, 14*, 21-38. https://www.researchgate.net/publication/317412296_THE_LITERATURE_REVIEW_OF_TECHNOLOGY_ADOPTION_MODELS_AND_THEORIES_FOR_THE_NOVELTY_TECHNOLOGY

41 Le, T. P. A., & Rajah, E. (2022). Using chatbots in customer service: A case study of Air New Zealand. https://www.unitec.ac.nz/epress/wp-content/uploads/2022/12/2021-RS-p161-176-Anh-Lee-Rajah.pdf

42 Lishchynska, D. (2022). How to Make Sure Your Chatbot Is GDPR Compliant. *BotsCrew*. https://botscrew.com/blog/how-to-make-your-chatbot-gdpr-compliant/

43 Lui, A., & Lamb, G. W. (2018). Artificial intelligence and augmented intelligence collaboration: regaining trust and confidence in the financial sector. *Information & Communications Technology Law, 27*(3), 267-283. https://researchonline.ljmu.ac.uk/id/eprint/8512/3/Artificial%20intelligence%20and%20augmented%20intelligence%20collaboration%20Regaining%20trust%20and%20confidence%20in%20the%20financial%20sector.pdf

44 Mcilraith, B. (2023). Latitude Financial cyberattack exposes the data of more than 300,000 customers in NZ and Australia. Stuff. https://www.stuff.co.nz/business/131524535/latitiude-financial-cyberattack-exposes-the-data-of-more-than-300000-customers-in-nz-and-austral

45 Mills, K. (1997). *ASB almost ready to roll on Internet banking*. Computerworld. https://www2.computerworld.co.nz/article/518668/asb_almost_ready_roll_internet_banking/

46 Misischia, C. V., Poecze, F., & Strauss, C. (2022). Chatbots in customer service: Their relevance and impact on service quality. *Procedia Computer Science, 201*, 421-428. https://reader.elsevier.com/reader/sd/pii/S1877050922004689?token=8B55E45C23DC9B481F6276A0422BD15FD6FE32D061FC94FA7E2B455E58DE28DDD92874842D7B7B0B6B27FAEE4B4714F1&originRegion=us-east-1&originCreation=20230224024440

47 Mixson, E. (2021). 3 Ways American Express is Using AI to Stay Ahead of Disruption. AI data Analytics & Networks. https://www.aidataanalytics.network/data-science-ai/articles/3-ways-american-express-is-using-ai-to-stay-ahead-of-disruption

48 Murphy, T. (2023). The evolution of chatbots and generative AI. https://www.techtarget.com/searchcustomerexperience/infographic/The-evolution-of-chatbots-and-generative-AI

49 New Zealand Herald. (2023). Chat GPT is being used by cybercriminals to generate scams, Norton warns, . https://www.nzherald.co.nz/business/chatgpt-being-used-by-cybercriminals-to-generate-scams-norton-warns/D3BT76RM4JFNFMY3NJVJSCMR2Y/

50 Newman, M. (2022). *Chatbots taking over big NZ business inquiries*. NZTECH. https://nztech.org.nz/2022/06/15/chatbots-taking-over-big-nz-business-inquiries/

51 NZTECH. (2019). *Chatbot or digital humans part of daily life in NZ*. https://nztech.org.nz/2019/11/07/chatbot-or-digital-humans-part-of-daily-life-in-nz/

52 Open AI. (2023). Privacy Policy, https://openai.com/policies/privacy-policy

53 Oruganti, S. C. (2020). Virtual bank assistance: An AI based voice bot for better banking. *International Journal of Research, 9*(1), 177-183. https://www.researchgate.net/profile/Sarath-Chandra-11/publication/339500060_VIRTUAL_BANK_ASSISTANCE_AN_AI_BASED_VOICE_BOT_FOR_BETTER_BANKING/links/5e564ab1299bf1bdb83b2c21/VIRTUAL-BANK-ASSISTANCE-AN-AI-BASED-VOICE-BOT-FOR-BETTER-BANKING.pdf

54 Paliwal, S., Bharti, V., & Mishra, A. K. (2020). Ai chatbots: Transforming the digital world. *Recent Trends and Advances in Artificial Intelligence and Internet of Things*, 455-482. https://link.springer.com/chapter/10.1007/978-3-030-32644-9_34

55 Paul, A. (2023). No, the AI chatbots (still) aren't sentient. *Popular Science*. https://www.popsci.com/technology/chatgpt-google-chatbot-sentient/

56 Pearce, G. (2021). *Beware the Privacy Violations in Artificial Intelligence Applications*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/beware-the-privacy-violations-in-artificial-intelligence-applications

57 Pickup, O. (2022). How financial services operators are dialling up conversational AI to catch out fraudsters. *Raconteur*. https://www.raconteur.net/technology/how-financial-services-operators-are-dialling-up-conversational-ai-to-catch-out-fraudsters/

58 Preveil. (2022). *What is end-to-end encryption & how does it work?* https://www.preveil.com/blog/end-to-end-encryption/

59 Raj, A. (2021). Are voice biometrics the unique gamechanger AI chatbots need? T_HQ technology and business. https://techhq.com/2021/07/are-voice-biometrics-the-unique-gamechanger-ai-chatbots-need/

60 Ravi, V., & Kamaruddin, S. (2017). Big data analytics enabled smart financial services: opportunities and challenges. In *Big Data Analytics: 5th International Conference, BDA 2017, Hyderabad, India, December 12-15, 2017, Proceedings 5* (pp. 15-39). Springer International Publishing. https://www.researchgate.net/publication/321282806_Big_Data_Analytics_Enabled_Smart_Financial_Services_Opportunities_and_Challenges

61 Sajan, K. (2022). *What are the privacy and security issues associated with chatbots?* Tutorialspoint. https://www.tutorialspoint.com/what-are-the-privacy-and-security-issues-associated-with-chatbots

62 Shalimov, A. (2022). Chatbots in FinTech: Benefits and best use cases for 2022. https://easternpeak.com/blog/chatbots-in-fintech-use-cases/

63 Shaqiri, B. (2021). Development and Refinement of a chatbot for Cybersecurity Support. https://files.ifi.uzh.ch/CSG/staff/franco/extern/theses/BA-B-Shaqiri.pdf

64 Sharma, S., Singh, G., Islam, N., & Dhir, A. (2022). Why Do SMEs Adopt Artificial Intelligence-Based Chatbots? I*EEE Transactions on Engineering Management*. https://ieeexplore.ieee.org/abstract/document/9908467

65 Shawar, B. A., & Atwell, E. (2007). Chatbots: are they really useful? *Journal for Language Technology and Computational Linguistics, 22*(1), 29-49. https://www.researchgate.net/publication/220046725_Chatbots_Are_they_Really_Useful

66 Singh, P. (2022). *Chatbots for Financial Services: Benefits, Examples, and Trends*. Reve Chat. https://www.revechat.com/blog/chatbots-for-financial-services/

67 Stewart, E. (2023). AI and GDPR: A Data Privacy Nightmare. *EM360 Enterprise Management 360*. https://em360tech.com/tech-article/ai-and-gdpr-data-privacy-nightmare

68 Sugumar, M., & Chandra, S. (2021). Do I desire chatbots to be like humans? exploring factors for adoption of chatbots for financial services. *Journal of International Technology and Information Management, 30*(3), 38-77. https://scholarworks.lib.csusb.edu/jitim/vol30/iss3/3/

69 Suta, P., Lan, X., Wu, B., Mongkolnam, P., & Chan, J. H. (2020). An overview of machine learning in chatbots. *International Journal of Mechanical Engineering and Robotics Research, 9*(4), 502-51. http://www.ijmerr.com/uploadfile/2020/0312/20200312023706525.pdf

70 Te Tari Taiwhenua Internal Affairs. (2021). *Te Tari Taiwhenua | Department of Internal Affairs*, https://www.dia.govt.nz/Identity---What-is-identity-theft

71 Tellols, D., Lopez-Sanchez, M., Rodríguez, I., Almajano, P., & Puig, A. (2020). Enhancing sentient embodied conversational agents with machine learning. *Pattern Recognition Letters, 129*, 317-323. https://diposit.ub.edu/dspace/bitstream/2445/192860/1/699595.pdf

72 Tiku, N. (2022). The Google engineer who thinks the company's AI has come to life. *The Washington Post, 11*. https://www.veritauniversale.it/wp-content/uploads/2023/01/Ingegnere-di-Google-che-pensa-che-lIA-dellazienda-abbia-preso-vita-e-viene-licenziato.pdf

73 Venugopal, V. (2023). Chatbot attacks: What are they and how to prevent them? *Softvire*. https://www.softvire.co.nz/chatbot-attacks-what-are-they-and-how-to-prevent-them/

74 Weißensteiner, A. A. A. (2018). Chatbots as an approach for a faster enquiry handling process in the service industry. *Signature, 12*(04). https://www.modul.ac.at/uploads/files/Theses/Bachelor/Undergrad_2018/Thesis_1511041_Alina_Weissensteiner_no_sig.pdf

75 Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning. ISBN: 9780357506431

76 Williams, P. (2022). My Fair LaMDA: Why Google's 'sentient' AI is not conscious, it's just another computer programme. *Premier Unbelievable Faith Explored*. https://www.premierunbelievable.com/articles/my-fair-lamda-why-googles-sentient-ai-is-not-conscious-its-just-another-computer-programme/13488.article