International Journal of
Financial Studies

MDPI

Article

Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust

Hassan H. H. Aldboush [1,*] and Marah Ferdous [2,*]

[1] Department of Finance & Banking, Faculty of Business, Philadelphia University, Amman 19392, Jordan
[2] Financial Technology and Accounting Analytics, School of Business Technology, Princess Sumaya University, P.O. Box 1438, Amman 11941, Jordan
* Correspondence: haldboush@philadelphia.edu.jo (H.H.H.A.); mar20228194@std.psut.edu.jo (M.F.)

Abstract: This research paper explores the ethical considerations in using financial technology (fintech), focusing on big data, artificial intelligence (AI), and privacy. Using a systematic literature-review methodology, the study identifies ethical and privacy issues related to fintech, including bias, discrimination, privacy, transparency, justice, ownership, and control. The findings emphasize the importance of safeguarding customer data, complying with data protection laws, and promoting corporate digital responsibility. The study provides practical suggestions for companies, including the use of encryption techniques, transparency regarding data collection and usage, the provision of customer opt-out options, and the training of staff on data-protection policies. However, the study is limited by its exclusion of non-English-language studies and the need for additional resources to deepen the findings. To overcome these limitations, future research could expand existing knowledge and collect more comprehensive data to better understand the complex issues examined.

Keywords: fintech; big-data analytics; artificial intelligence (AI); data security and privacy; corporate digital responsibility (CDR); customer trust; ethical considerations

Citation: Aldboush, Hassan H. H., and Marah Ferdous. 2023. Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. *International Journal of Financial Studies* 11: 90. https://doi.org/10.3390/ijfs11030090

Academic Editors: Muneer M. Alshater and Rim El Khoury

Received: 8 April 2023
Revised: 17 May 2023
Accepted: 30 May 2023
Published: 10 July 2023

1. Introduction

Fintech businesses have used big-data analytics and artificial intelligence (AI) to evaluate enormous volumes of data from several sources and to make autonomous suggestions or judgments (Li et al. 2022; Yu and Song 2021). Fintech organizations may provide more individualized financial services, increase operational effectiveness, and cut costs by integrating AI and big data (Ashta and Herrmann 2021). ChatGPT, as an AI tool, plays a crucial role in this context by assisting in the analysis of big data and enabling fintech organizations to provide more personalized financial services, enhance operational effectiveness, and reduce costs (George and George 2023). However, the integration of AI and big data also brings forth ethical and privacy concerns, encompassing issues of bias, discrimination, privacy, transparency, justice, ownership, and control (Hermansyah et al. 2023). The complexity of the financial system and the internal data representations of AI systems may pose challenges for human regulators in effectively addressing emerging problems (Butaru et al. 2016). Therefore, an understanding of the ethical implications of fintech, including the responsible use of tools such as ChatGPT, is paramount in fostering customer trust and confidence (George and George 2023).

This study aims to investigate the ethical issues surrounding fintech, particularly those in which big data, AI, and privacy are concerned. It focuses on resolving data-security and privacy issues while examining the intricate interplay between fintech and customer trust. A summary of the best practices and approaches for adhering to data-privacy rules and regulations, as well as corporate digital responsibility for boosting financial success and digital trust, are also provided by this research. The exploration of the ethical implications

of fintech and how they affect digital trust, customer acceptance of fintech services, and how to earn customers' confidence are the driving forces behind the study.

This study's objectives strongly emphasize the value of safeguarding customer data, calling for firms to gather and utilize customer data responsibly, uphold reliable data-security measures, use encryption techniques, and routinely evaluate and update their data-protection policies. Organizations must be transparent about their data-collection and -usage processes, allowing customers to opt out of data collection and use and follow data-protection laws and regulations. Companies must also ensure that their data sets are diverse and represent their customer base to prevent discriminatory practices. Additionally, organizations must provide their staff with appropriate training related to customer-data protection and hold them accountable for following established policies and procedures. Therefore, this research paper investigates the ethical implications of the integration of big data and AI in the financial sector. The paper addresses the following research questions: (1) What are the ethical implications of the integration of big data and AI in the financial sector, and how can issues such as bias, discrimination, privacy, transparency, justice, ownership, and control be addressed? (2) How do data-privacy and -security concerns affect customer trust in fintech companies, and which strategies can be implemented to resolve these issues? (3) What are the best practices and approaches for adhering to data-privacy rules and regulations in the digital finance industry, and how can organizations ensure compliance with data-protection laws and regulations? (4) What is the impact of the corporate digital responsibility (CDR) culture on financial performance and digital trust, and which indirect performance benefits, such as customer satisfaction, competitive advantage, customer trust, loyalty, and company reputation, are associated with it?

The study's findings suggest that inadequate internal controls are leading causes of fraud and asset misappropriation in firms, and millennials are more vulnerable to privacy risks regarding online banking due to their significantly lower level of financial knowledge than older generations. Studies have also demonstrated that businesses with a corporate digital responsibility (CDR) culture benefit from indirect performance effects, such as customer satisfaction, competitive advantage, customer trust, loyalty, and company reputation.

This paper contributes to the literature by examining the ethical and privacy considerations associated with the intersection of big data, AI, and privacy in the digital finance industry. It considers the complex relationship between fintech and customer trust and provides best practices and strategies for organizations to ensure compliance with data-protection laws and regulations. This study acknowledges the importance of digital trust in the adoption of fintech services and explores the impact of data-privacy and -security concerns on customers' trust in fintech companies. Finally, the study emphasizes the importance of corporate digital responsibility in enhancing financial performance and digital trust. It argues that businesses with a CDR culture benefit from indirect performance effects, such as customer satisfaction, competitive advantage, customer trust, loyalty, and company reputation.

2. Methodology

The current study employed a systematic review method to establish a reliable evidence base for recommendations to schools, teachers, and CPD providers. The systematic-review process is defined as "a scientific process governed by a set of explicit and demanding rules oriented towards demonstrating comprehensiveness, immunity from bias, and transparency and accountability of technique and execution" (Dixon-Woods 2011, p. 332). The review included empirical research published since 2005 and involved a range of approaches, including searching academic journals, library catalogs, and online databases. The search strategy incorporated specific keywords related to the research topic, such as "FinTech," "Big data analytics," "Artificial intelligence (AI)," "Data security and privacy," "Corporate digital responsibility (CDR)," "Customer trust," and "Ethical considerations." Through this rigorous process, a total of 39 relevant studies were identified and

included in the review. The systematic-review process (Figure 1) involved the following steps (Dixon-Woods 2011):

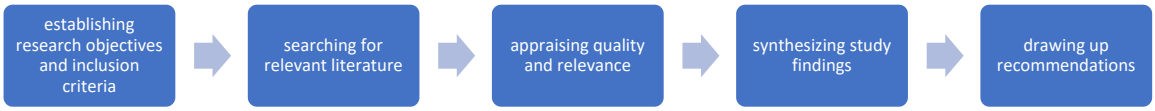

Figure 1. Systematic review process.

Each process step was documented, and choices were made as a team to ensure the evaluation was methodical. The initial step involved defining the inclusion criteria, which mandated the selection of peer-reviewed research written in English that directly aligned with the research goals. Additionally, exclusion criteria were established to exclude studies lacking authenticity, dependability, or relevance to the research objectives. These criteria underwent refinement to ensure the selection of high-quality and relevant papers for analysis. Subsequently, an extensive search was conducted across multiple databases and sources using predefined search terms and keywords. The databases utilized included Google Scholar, ACM, Springer, Elsevier, Emerald, Web of Science, MDPI, and Scopus to encompass a wide range of sources. Subject-matter experts were approached to address questions about the suitability of the search keywords, and their recommendations were integrated to ensure thoroughness and relevance.

After identifying potentially relevant studies, each study underwent an appraisal to assess its quality, relevance, and methodological rigor concerning the research questions. Various methods and techniques, such as checklists, were employed to ensure consistency and reliability during the appraisal process. The findings of the selected studies were then synthesized by organizing the summaries of research methodology, findings, and weight of evidence under thematic headings. This process facilitated the organization of findings and the identification of key themes and patterns in the literature. Each piece of research was carefully screened against the inclusion criteria, mapped, and summarized before it was synthesized into the report. The findings were appraised regarding their methodological quality and relevance to derive reliable and valid conclusions. Techniques such as statistical analysis and data visualization were employed to enhance the understanding and presentation of the findings.

Ultimately, a set of recommendations closely linked to the synthesized findings was formulated, identifying the practical implications of the research for future studies and practice. A rigorous and systematic process underpinned the research paper to ensure the inclusion of high-quality studies that directly aligned with the research objectives.

Content analysis was employed to identify the research themes and topics discussed in the literature, as well as to identify gaps. This involved analyzing the content of research papers and utilizing ChatGPT's natural-language-processing tool to classify streams and sub-streams. Initially, a sample of research papers was uploaded to the tool for content analysis, generating a list of suggested themes and sub-themes. Subsequently, a manual review-and-refinement process was conducted to ensure their relevance to the research questions. Experts in natural language processing were consulted to validate the suitability of the tool for this analysis. A rigorous data-collection-and-analysis process was implemented to ensure high-quality and pertinent data utilization. Once the themes and sub-themes were identified, selected research findings within each theme were thoroughly reviewed to identify critical research gaps. This comprehensive process enhanced the understanding of the current state of research in the field and highlighted areas that require further investigation.

To summarize, a systematic-review methodology was employed to establish a reliable evidence base for providing recommendations to schools, teachers, and CPD providers. The methodology involved various steps, including definition of inclusion and exclusion criteria, performance of comprehensive database searches, appraisal of study quality and relevance, synthesis of findings, and formulation of recommendations. Statistical analysis and data

visualization were used to present the findings, while content analysis was employed to identify research themes and gaps in the literature. The review and analysis were grounded in high-quality and pertinent data, and expert consultation in natural language processing ensured the appropriateness of the analysis tool. This study's rigorous and systematic methodology ensured a comprehensive, transparent, and accountable review-and-analysis process. The recommendations derived from the synthesis were closely aligned with the findings, establishing practical implications for future research and practice. In essence, the methodology employed in this study aimed to provide a robust evidence base for informing individuals, organizations, and fintech providers. The utilization of natural-language-processing tools, such as ChatGPT, facilitated the efficient and effective analysis of a substantial volume of research, identifying crucial research gaps in the field.

Overall, this study adhered to a rigorous systematic approach that met high quality standards and addressed the research objectives directly. The integration of various methods, techniques, and expert consultations contributed to the study's comprehensive nature, enhancing the findings' reliability and validity. By following this well-structured methodology, the study aimed to provide a solid foundation of evidence to guide decision-making and future investigations in the field.

3. Literature Review

The fintech industry has witnessed significant advancements in recent years, fueled by digitalization and the integration of big-data analysis, artificial intelligence (AI), and cloud computing (Lacity and Willcocks 2016). As a result, banks and financial institutions are able to offer more convenient and adaptable services to customers through financial technology (fintech) (Malaquias and Hwang 2019). By leveraging mobile devices and other technological platforms, fintech enables customers to easily access their bank accounts, receive transaction notifications, and engage in various financial activities (Stewart and Jürjens 2018b).

One of the key drivers of the adoption of AI in the fintech sector is its ability to process vast amounts of data and extract valuable insights for decision-making purposes (Daníelsson et al. 2022). With the integration of AI and big-data analytics, fintech companies can offer personalized financial services, enhance operational efficiency, and reduce costs, thereby gaining a competitive edge in the market (Peek et al. 2014; Mars and Gouider 2017). However, the use of AI and big data in the fintech industry raises ethical and privacy concerns (Matzner 2014; Yang et al. 2022).

The intersection of big data, AI, and privacy in the fintech sector has prompted discussions on the importance of addressing ethical considerations. These considerations include bias, discrimination, privacy, transparency, justice, ownership, and control (Saltz and Dewar 2019). Ensuring fairness in decision-making processes is crucial, as biased or incomplete data inputs can lead to unfair or discriminatory outcomes that significantly affect individuals (Daníelsson et al. 2022). Transparency in data collection, processing, and analysis is also essential for maintaining customer trust and credibility (Vannucci and Pantano 2020). Moreover, the protection of personal data and adherence to data-protection laws and regulations are critical ethical considerations for fintech companies (La Torre et al. 2019).

The complex relationship between fintech and customer trust is another significant aspect that requires attention. Trust plays a pivotal role in the adoption of fintech services, particularly concerning data security and privacy (Stewart and Jürjens 2018b). Online-banking vulnerabilities and data breaches have raised concerns among customers, making them cautious about engaging in financial transactions through fintech platforms (Swammy et al. 2018). Addressing data privacy and security concerns is essential for fostering customer trust and encouraging the broader adoption of fintech services (Laksamana et al. 2022).

To bridge the trust gap in the fintech era, strategies for fostering trust in fintech companies have been proposed. One such strategy is the adoption of corporate digital

responsibility (CDR), which emphasizes the responsible and ethical use of data and technological innovations (Jelovac et al. 2021). The implementation of a culture of CDR within organizations can enhance financial performance, digital trust, customer satisfaction, and reputation (Saeidi et al. 2015). By prioritizing the positive impact of technology on society and ensuring ethical data processing, fintech companies can establish and maintain digital trust (Herden et al. 2021).

Furthermore, compliance with data-protection laws and regulations is crucial in ensuring data privacy and security in the digital finance industry. The General Data Protection Regulation (GDPR), implemented in the European Union (EU), has emerged as a significant framework for data privacy and protection (Mars and Gouider 2017). The GDPR mandates that organizations handling personal data must obtain explicit consent from individuals, provide transparent information about data processing, and implement appropriate security measures. Compliance with the GDPR safeguards customer data and enhances trust and credibility in the fintech sector (Vannucci and Pantano 2020).

In addition to regulatory compliance, embracing technological solutions is crucial for effectively protecting customer data in the fintech industry. Encryption algorithms, for example, play a vital role in ensuring that sensitive information remains unreadable and secure during transmission and storage (Peek et al. 2014). By employing strong encryption techniques, fintech companies can prevent unauthorized access to customer data and mitigate the risk of data breaches. Moreover, the implementation of multi-factor authentication methods, such as biometrics or token-based systems, adds an extra layer of security to customer accounts and reduces the likelihood of unauthorized access (Yang et al. 2022).

Addressing ethical and privacy challenges in the fintech sector requires collaborative efforts among various stakeholders. Fintech companies, regulators, and consumers must work together to establish ethical guidelines, promote responsible data practices, and enhance transparency (Gong et al. 2020). Regulatory bodies play a crucial role in monitoring the evolving landscape of fintech and in adapting policies and guidelines accordingly to protect consumer rights and privacy (Castellanos Pfeiffer 2019).

Fintech companies, for their part, should adopt transparent practices, educate customers about data privacy, and provide clear opt-out mechanisms to respect individual autonomy (Swammy et al. 2018).

In conclusion, the integration of AI and big data in the fintech industry presents opportunities and challenges. While these technologies enable innovative financial services and enhanced customer experiences, addressing ethical concerns such as bias, transparency, privacy, and trust is paramount. By prioritizing the responsible and ethical use of data, complying with regulatory frameworks such as the GDPR, and adopting secure technological solutions, fintech companies can build trust, ensure customer privacy, and foster the industry's sustainable growth. Collaborative efforts between stakeholders are crucial in creating an ethical and privacy-conscious fintech ecosystem.

4. Content Analysis

This research paper reports a content analysis of data-privacy vulnerabilities in the fintech industry. A thematic-analysis approach was utilized to categorize the collected research into three key themes. The first theme, Ethical Considerations in Fintech: The Intersection of Big Data, AI, and Privacy, highlights the significance of addressing concerns such as bias, discrimination, privacy, transparency, justice, ownership, and control in the fintech sector. The second theme, Navigating the Complex Relationship between Fintech and Customer Trust: Addressing Data-Privacy and -Security Concerns, underscores the need to address data-security and -privacy issues to cultivate customer trust in fintech companies. The third theme, Bridging the Trust Gap: Strategies for Fostering Trust in the Fintech Era, offers strategies for building trust in fintech companies by promoting corporate digital responsibility and adherence to data-privacy laws and regulations. The findings of

this analysis highlight the critical role of data privacy and security in building customer trust and corporate reputation.

Furthermore, the paper suggests best practices and strategies for fintech companies to ensure data protection and security. The implications of these findings are relevant to financial firms, policymakers, and other stakeholders seeking to ensure the responsible and ethical use of big data and AI in the digital finance industry. Nevertheless, it is essential to expand on the study's limitations, such as the exclusion of non-English language studies and the need for additional resources to deepen the findings. By collecting more comprehensive data and expanding existing knowledge, researchers can better understand the complex ethical and privacy issues associated with fintech.

4.1. Ethical Considerations in Fintech: The Intersection of Big Data, AI, and Privacy

The advancement of digitalization, supported by technical enablers such as big-data analysis, cloud computing, mobile technologies, and integrated sensor networks, is causing significant changes in how organizations operate in economic sectors (Lacity and Willcocks 2016). With increased internet and e-commerce usage, banks can now provide customers with more convenient, effective, and adaptable services (Malaquias and Hwang 2019). This has led to the utilization of financial technology (fintech) to enhance banking services through the use of mobile devices and other technological platforms to access bank accounts, receive transaction notifications, and debit and credit alerts through push notifications via APP, SMS, or other notification types. Fintech also includes mobile-application features such as multi-banking, blockchain, fund transfer, robot advisory, and concierge services, from payments to wealth management (Stewart and Jürjens 2018b).

To improve the speed and accuracy of their operations, deliver personalized services to customers, and reduce expenses, fintech companies have leveraged artificial intelligence (AI). This is a technology that replicates cognitive functions associated with humans and facilitates the processing of vast amounts of data generated from multiple sources, such as social media, online transactions, and mobile applications (Daníelsson et al. 2022). Algorithms based on AI use significant data inputs and outputs to recognize patterns and effectively "learn" to train machines to make autonomous recommendations or decisions. The implementation of AI allows fintech companies to extract valuable insights to support their decision-making processes through big-data analytics. Big data refers to an overwhelming influx of data from numerous sources in various formats, representing significant challenges for conventional data-management methods (Peek et al. 2014; Mars and Gouider 2017). In the financial market, big data has become a critical asset that is used to record information about individual and enterprise customers (Erraissi and Belangour 2018). By integrating AI and big data, fintech companies can provide more personalized financial services, improve operational efficiency, and reduce costs, enhancing their competitive edge in the market. However, this raises ethical and privacy challenges (Castellanos Pfeiffer 2019; Gong et al. 2020; Yang et al. 2022).

The use of AI in the Internet of Things (IoT) context raises ethical, security, and privacy concerns. The lack of intelligibility of the financial system and internal data representations of AI systems may impede human regulators' ability to intervene when issues arise (Butaru et al. 2016). Systems based on AI rely on data inputs that may be biased or incomplete in determining individuals' preferences for services or benefits, resulting in unfair or discriminatory decisions that can significantly affect individuals. Additionally, AI algorithms can potentially threaten data privacy by collecting and analyzing large amounts of personal data without individuals' knowledge or consent, which can be used for various purposes, including targeted advertising or political profiling. These risks raise significant concerns about the potential for data misuse and the erosion of privacy. The collection and processing of large amounts of personal data can pose privacy threats, including data misuse and the erosion of privacy, if the data are not collected and stored in compliance with data-protection laws and regulations (Vannucci and Pantano 2020). The de-identification of data to protect an individual's privacy while allowing meaningful analysis

is another challenge in big-data analytics (La Torre et al. 2019). The ethical considerations surrounding big data include privacy, fairness, transparency, bias, and ownership, and control (Saltz and Dewar 2019). The protection of personal information and its use in a transparent, reasonable, and respectful manner is crucial to ensuring data privacy. This is especially important in the financial industry, in which sensitive information such as bank-account numbers, credit scores, and transaction details are involved.

Fairness in decision-making is another critical consideration when using big data and AI algorithms. As Daníelsson et al. (2022) noted, biased or incomplete data inputs can result in unfair or discriminatory decisions that significantly affect individuals. To address this issue, fintech companies must ensure that their data sets are diverse and represent their customer base. They should also implement ethical and unbiased data-processing methods to prevent discrimination and ensure fairness in decision making. Transparency in data collection, processing, and analysis is crucial for maintaining customer trust and credibility. Fintech companies should clearly and concisely explain how they collect, store, and use personal data. Additionally, they should be transparent about their algorithms and the decision-making processes behind their services. Finally, the ownership and control of personal data are critical ethical considerations that fintech companies must address. They must adhere to data-protection laws and regulations to protect the rights and interests of data owners. This includes obtaining consent before collecting and using personal data and ensuring that data are deleted securely and promptly when no longer needed.

In conclusion, the integration of AI and big data in fintech services provides significant benefits, such as improved efficiency, personalized services, and reduced costs. However, this also raises ethical and privacy concerns that must be addressed to protect customers' rights and interests. By implementing ethical data-processing methods, ensuring transparency, and respecting data ownership and control, fintech companies can enhance their reputations and maintain trust with their customers.

4.2. Navigating the Complex Relationship between Fintech and Customer Trust: Addressing Data-Privacy and-Security Concerns

The impact of financial technology, or fintech, on the retail-banking sector has been extensively researched and debated in recent years. Yousafzai et al. (2005) found that fintech has enabled banks to provide their customers with more convenient, effective, and adaptable services through mobile-banking apps and online payment systems, which enhance overall customer experience and provide greater accessibility to financial transactions. However, the entry of fintech companies to the market and their offers of alternative financial services have sparked concerns about data privacy and security and the impact of competition on service quality (Malaquias and Hwang 2019).

The adoption of digital products and services by individuals and firms from financial institutions is heavily influenced by the perceived trustworthiness of the provider (Fu and Mishra 2022). Trust in financial institutions, mainly traditional incumbents, was eroded after the global financial crisis, leading to a shift towards fintech (Goldstein et al. 2019, as cited in Fu and Mishra 2022). However, online banking has inherent vulnerabilities that expose users to various risks (Stewart and Jürjens 2018a), and trust is critical in risky situations. Stewart and Jürjens (2018b) noted that information-security components such as confidentiality, integrity, availability, authentication, accountability, assurance, privacy, and authorization influence customers' trustworthiness. Therefore, fintech adoption is influenced by customer trust, data security, user-interface design, technical difficulties, and a lack of awareness or understanding of the technology (Abidin et al. 2019).

Millennials, born between 1980 and 2000, considered the most influential generation in consumer spending, comprise a significant portion of online-banking customers. They are more likely to share personal information through social media and online platforms for financial transactions, increasing their risk of information misuse. In addition, millennials have a significantly lower level of financial knowledge than older generations, making them more vulnerable to privacy risks regarding online banking (Liyanaarachchi et al. 2021).

Privacy in online banking is defined as the potential for loss due to fraud or a hacker compromising the security of an online bank user (Liyanaarachchi et al. 2021). With many customers finding fintech convenient and practical, customers less familiar with fintech are more skeptical and concerned about potential risks and negative effects (Swammy et al. 2018).

Many consumers are cautious about and reluctant to engage in online banking transactions due to concerns about the security of their personal information, as most data breaches and identity thefts occur in online banking environments (Stewart and Jürjens 2018a). Fintech firms must address data-security and -privacy concerns to increase client confidence and trust, in order to ensure the broader adoption and acceptance of fintech services (Laksamana et al. 2022). Therefore, banks and financial-service providers should provide transparent information about their security measures, address technical issues that may arise, and provide customer support. By addressing these factors, banks and other financial-service providers can help to build trust and confidence among their customers and encourage the broader adoption of e-banking (Moscato and Altschuller 2012).

4.3. Bridging the Trust Gap: Strategies for Fostering Trust in the Fintech Era

4.3.1. Corporate Digital Responsibility: Enhancing Financial Performance and Digital Trust through Ethical and Responsible Data Processing

New technologies have led to new social challenges and increased corporate responsibilities, particularly in digital technologies and data processing. As a result, the concept of corporate digital responsibility (CDR) has been introduced. The concept refers to various practices and behaviors that aid organizations in using data and technological innovations morally, financially, digitally, and ecologically responsible (Jelovac et al. 2021). Essentially, CDR is the recognition and dedication on the part of organizations to prioritize the favorable impact of technology on society in all aspects of their operations (Herden et al. 2021). The implementation of a culture of CDR can assist organizations in navigating the complex ethical and societal issues that arise with digital technologies and data processing (Lobschat et al. 2021). Studies have shown that businesses with a CDR culture benefit from indirect performance effects, resulting in a positive long-term financial impact, including customer satisfaction, competitive advantage, customer trust, loyalty, and enhanced company reputation (Saeidi et al. 2015). Therefore, organizations can enhance their financial performance, brand equity, and marketability (Lobschat et al. 2021). In the digital age, trust is a critical factor, particularly trust in digital institutions, technologies, and platforms, referred to as digital trust. Trust is "our readiness to be vulnerable to the actions of others because we believe they have good intentions and will treat us accordingly." Digital trust is associated with trust in digital institutions, digital technologies, and platforms; it refers to users' trust in the ability of digital institutions, companies, technologies, and processes to create a safe digital world by safeguarding users' data privacy (Jelovac et al. 2021).

Creating a digital society and economy is contingent upon all participants having high trust. Digital trust is founded on convenience, user experience, reputation, transparency, integrity, reliability, and security, which control stakeholders' data. The adoption of a culture of CDR within modern businesses and organizations is necessary to establish and maintain digital trust. This offers numerous benefits to companies, including the shaping of their future, the development and maintenance of positive, long-term relationships with stakeholders, improvements in reputation, the creation of competitive advantage, and increases in employee cohesion and productivity (Herden et al. 2021).

Corporate digital responsibility entails organizations' comprehension of and commitment to the prioritization of technology's positive impact on society in all aspects of their business (Herden et al. 2021). As a result, CDR contributes to digital trust through corporate reputation disclosures (CRDs). These provide information about a company's products and services, vision and leadership, financial performance, workplace environment, social and environmental responsibility, emotional appeal, and prospects and public reputation (Baumgartner et al. 2022). Therefore, CDR acts as a signal to decrease the information asymmetry between managers and stakeholders and allows stakeholders to

evaluate a company's ability to meet their needs, as well as its reliability and trustworthiness (Baumgartner et al. 2022).

4.3.2. Ensuring Data Privacy and Security in the Digital Finance Industry: Best Practices and Strategies for Compliance with Data-Protection Laws and Regulations

The protection of individuals' personal data through compliance with data-privacy laws and regulations is crucial in the digital finance industry. The General Data Protection Regulation (GDPR) gives individuals specific rights regarding their data, such as access to these data, the right to be informed about their collection and use, and the right to have them erased (Ayaburi 2022). Businesses must take necessary measures to protect personal data and obtain explicit consent from individuals for their processing in specific circumstances.

To ensure compliance with data-protection laws and regulations, companies must take several steps to protect against data-privacy breaches. These steps include the implementation of encryption and secure authentication protocols, de-identification techniques, and regular reviews and the establishment of data-protection policies (Beg et al. 2022). Data-governance frameworks can ensure ethical and responsible big-data management by outlining roles and responsibilities, data-handling practices, and compliance procedures (Stewart and Jürjens 2018a). Regular audits, employee training on data-protection practices, and procedures for detecting and addressing data-privacy breaches are also essential (Abidin et al. 2019). When using AI systems, careful data analysis and privacy-preserving machine-learning techniques are necessary to prevent confounding bias and illegal access to personal data (Abed and Anupam 2022).

Employee responsibility and accountability are crucial in organizations' information security and data protection. A lack of adequate internal controls has been identified as a cause of fraud and asset misappropriation in firms (Lokanan 2014). To prevent customer-data theft, companies must prioritize employee training, carefully recruit staff, monitor customer data, oversee third-party access, use advanced technology, and prevent unauthorized access to data. The factors contributing to data theft include staff stealing customer data, noncompliance with customer-data-protection policies, a lack of knowledge about data-protection duties and procedures, and ignorance of client-data-protection procedures (Abidin et al. 2019).

Leadership is critical in ensuring data privacy and security within organizations. Leaders can address privacy concerns, build trust through effective sales and marketing strategies, and manage online banking platforms to encourage interactions that enhance confidentiality and trust, leading to a competitive advantage (Liyanaarachchi et al. 2020). To ensure data protection, leaders must obtain customers' consent regarding their data, take concrete precautions to protect these data, and delete them when they are no longer required (Abidin et al. 2019). Additionally, leaders must ensure that staff members are trained in data-protection procedures and held accountable for following them, as well as creating protocols for identifying and responding to data-privacy breaches (Liyanaarachchi et al. 2021).

The study by Abidin et al. (2019) found that 56% of staff members at ABC Bank Services needed appropriate training related to customer-data protection for their job functions and responsibilities. This finding suggests ineffective communication channels and poor monitoring by senior management, leading to the need for a better understanding of the latest customer-data-protection policies and procedures. Overall, the primary goals of data-protection activities are to maintain a state of security and control security risks throughout an organization (La Torre et al. 2019). Organizations must comprehend the risks involved and establish who is responsible for data protection to safeguard against data breaches and maintain their clients' trust. This requires the understanding that protecting an organization's data involves more than determining whether privacy is a right or a commodity.

5. Results and Discussion

In this study, we conducted a content analysis of the literature to investigate the ethical and privacy considerations associated with the intersection of big data, artificial intelligence (AI), and privacy in the digital finance industry. A thematic analysis was used to identify three major themes:

5.1. Ethical Considerations in Fintech: The Intersection of Big Data, AI, and Privacy

This theme focuses on the ethical concerns raised by the integration of big data and AI in the financial sector, highlighting the need to address issues such as bias, discrimination, privacy, transparency, justice, ownership, and control.

5.2. Navigating the Complex Relationship between Fintech and Customer Trust: Addressing Data Privacy and Security Concerns

This theme examines the intricate interplay between fintech and customer trust, emphasizing the importance of resolving data-security and privacy issues. It calls for firms to gather and utilize customer data responsibly, maintain reliable data-security measures, and comply with data-protection laws and regulations.

5.3. Bridging the Trust Gap: Strategies for Fostering Trust in the Fintech Era

This theme offers strategies for building trust in fintech companies and consists of two sub-themes, which are described below.

5.3.1. Corporate Digital Responsibility: Enhancing Financial Performance and Digital Trust through Ethical and Responsible Data Processing

This sub-theme emphasizes the importance of a culture of corporate digital responsibility (CDR) in enhancing financial performance and digital trust. It highlights indirect performance benefits, such as customer satisfaction, competitive advantage, customer trust, loyalty, and company reputation.

5.3.2. Ensuring Data Privacy and Security in the Digital Finance Industry: Best Practices and Strategies for Compliance with Data-Protection Laws and Regulations

This sub-theme presents best practices and approaches for adhering to data-privacy rules and regulations, emphasizing the need to safeguard customer data, utilize encryption techniques, and regularly evaluate and update data-protection policies. It also calls for companies to be transparent about their data-collection and -usage processes and to provide their staff with appropriate training related to customer-data protection.

5.4. Results Tables

This section provides a performance analysis of the three major themes that emerged from our thematic analysis of the literature on ethical and privacy considerations in the digital finance industry. Table 1 presents the performance analysis of the first theme, Ethical Considerations in Fintech: The Intersection of Big Data, AI, and Privacy, which highlights the importance of addressing concerns such as bias, discrimination, privacy, transparency, justice, ownership, and control. Table 2 provides the performance analysis of the second theme, Navigating the Complex Relationship between Fintech and Customer Trust: Addressing Data-Privacy and -Security Concerns, which emphasizes the need to resolve data-security and -privacy issues to foster customer trust in fintech companies. Table 3 offers the performance analysis of the third theme, Bridging the Trust Gap: Strategies for Fostering Trust in the Fintech Era, which presents strategies for building trust in fintech companies, including the importance of corporate digital responsibility and adhering to data-privacy laws and regulations. Our analysis offers insights into the sector's main privacy issues and suggestions for managing them. Our findings have implications for financial firms, policymakers, and other stakeholders seeking to ensure the responsible and ethical use of big data and AI in the digital finance industry.

Table 1. Results—Ethical Considerations in Fintech: The Intersection of Big Data, AI, and Privacy.

Stream	Main Findings	Implications	Recommendations
Ethical Considerations in Fintech: The Intersection of Big Data, AI, and Privacy	1. The use of AI in the Internet of Things (IoT) can lead to potential ethical, security, and privacy concerns. While AI can enhance speed and accuracy and provide personalized services, it can also rely on biased or incomplete data, and it can be utilized to make unfair or discriminatory decisions. Moreover, AI may threaten data privacy by collecting and analyzing personal data without proper consent, potentially leading to data misuse. 2. The use of big data in the financial market is necessary but poses significant challenges to data privacy and security. There are risks of de-identification and re-identification, as well as risks of data misuse and the erosion of privacy. Inadequate data protection can lead to data breaches and identity theft, which can have severe consequences for individuals and organizations. 3. The increase in the global data volume makes data management and protection difficult, and it requires companies to develop robust data-management and -protection strategies to safeguard their data. 4. The use of big data in the financial market also presents challenges in risk management, which necessitates the implementation of effective risk-management strategies to address potential risks and ensure the responsible and ethical use of big data.	1. Companies that use AI must carefully consider the potential ethical, security, and privacy implications of their systems. 2. The failure to address data-privacy and -security challenges can compromise financial information and stability. 3. There are significant risks associated with data misuse and the erosion of privacy, which can lead to data breaches and identity theft. 4. Data management and protection can be complex and require careful consideration. 5. Companies must be prepared to address the challenges associated with risk management when implementing AI systems.	To ensure the responsible and ethical use of artificial intelligence (AI) and address potential ethical and privacy concerns, companies should take the following measures: 1. Implement protocols for fairness, transparency, and data security in AI systems. 2. Protect personal and sensitive data through, for example, encryption and access controls. 3. Secure and de-identify data to protect privacy and prevent unauthorized access. 4. Comply with applicable data-protection laws and regulations. 5. Develop comprehensive data-management and -protection strategies, including processes for data collection, storage, and use. 6. Address challenges related to risk management in AI implementation. By taking these steps, companies can promote the ethical and responsible use of AI while protecting the privacy and security of their stakeholders and customers.

Table 2. Results—Navigating the Complex Relationship between Fintech and Customer Trust: Addressing Data-Privacy and -Security Concerns.

Stream	Main Findings	Implications	Recommendations
Navigating the Complex Relationship between Fintech and Customer Trust: Addressing Data-Privacy and -Security Concerns	1. Fintech has improved the overall customer experience in retail banking by enabling banks to offer more convenient and effective services to customers. 2. The entry of fintech companies into the retail-banking sector has increased competition, leading to pressure on banks to lower prices and reduce margins. This may potentially decrease service quality. 3. Fintech has raised concerns about data privacy and security. To address these concerns, strong data-protection measures need to be formulated. 4. Trust is a critical factor in the adoption of fintech products and services. 5. Consumers who are less familiar with fintech may be more skeptical and concerned about potential risks and negative effects. 6. The key attributes that affect the acceptance and use of fintech include customer trust, data security, and user-design interfaces. 7. While consumers generally have positive attitudes towards e-banking, factors such as perceived risk, trust, and technical difficulties can influence adoption.	1. Fintech has brought about positive changes to the customer experience in the banking industry, but it has also intensified competition among banks. 2. It is crucial for banks to strike a balance between maintaining competitiveness and preserving service quality to avoid a potential decline in the latter. 3. Data privacy is a vital concern for both consumers and banks in the fintech industry, and appropriate measures must be taken to safeguard sensitive data. 4. Fintech companies need to work towards building trust with their customers to enhance the adoption and acceptance of their services. 5. Addressing data-security and -privacy concerns is key to building customer trust in fintech companies. 6. The design and usability of fintech products and services can significantly influence their acceptance and adoption by consumers.	1. Banks should prioritize customer experience and convenience while maintaining robust data-protection measures to ensure the privacy and security of customer data. 2. Fintech companies should prioritize building trust with their customers by addressing data-privacy and -security concerns and ensuring transparency in their operations. 3. Banks and financial-service providers should provide clear and transparent information about their security measures, promptly address technical issues, and offer reliable customer support to increase trust and confidence in e-banking.

Table 3. Results—Bridging the Trust Gap: Strategies for Fostering Trust in the Fintech Era.

Stream	Sub-Stream	Main Findings	Implications	Recommendations
Bridging the Trust Gap: Strategies for Fostering Trust in the Fintech Era	Corporate Digital Responsibility: Enhancing Financial Performance and Digital Trust through Ethical and Responsible Data Processing	1. Digital trust is a critical factor in the development of a digital society and economy, encompassing trust in digital institutions, technologies, and platforms. 2. Digital trust is essential for building and maintaining positive, long-term relationships with stakeholders. 3. Convenience, user experience, reputation, transparency, integrity, reliability, and security are key attributes of Digital trust that must be considered and maintained by stakeholders.	1. Emphasizing digital trust can help companies and organizations build and maintain positive relationships with consumers, as well as improving their reputation. 2. A lack of digital trust can damage relationships with stakeholders and hinder the development of a digital society and economy. 3. To ensure digital trust, companies must prioritize corporate digital responsibility (CDR), which involves the use of ethical and responsible practices in the development and use of digital technologies, as well as the promotion of social, economic, technological, and ecological responsibility.	1. To build and maintain digital trust, companies and organizations should prioritize the development of a culture of corporate digital responsibility (CDR). 2. CDR involves the adoption of ethical and responsible practices when using data and digital technologies, as well as ensuring that they are used in a socially, economically, technologically, and ecologically responsible way. iii. To build digital trust, companies and organizations should prioritize transparency, integrity, and security in their use of data and digital technologies. 3. To enhance digital trust, companies and organizations should provide clear and transparent information about their products, services, and practices through corporate reputation disclosures (CRDs) that are easily accessible to stakeholders.

Table 3. *Cont.*

Stream	Sub-Stream	Main Findings	Implications	Recommendations
	Ensuring Data Privacy and Security in the Digital Finance Industry: Best Practices and Strategies for Compliance with Data Protection Laws and Regulations.	1. Data theft is often caused by a combination of internal control weaknesses and employee-related factors. ii. Data-protection practices are frequently overlooked in favor of technological controls, leading to potential vulnerabilities. 2. Corporate-governance structures and stakeholder responsibility play crucial roles in ensuring effective data protection. 3. Employees' awareness and understanding of data protection are critical factors influencing data-protection practices. 4. Effective leadership is critical to ensure data privacy and security within organizations. ii. Online firms must prioritize addressing consumers' privacy concerns and build trust through effective sales and marketing strategies. 5. To ensure data protection, leaders must obtain customers' consent, secure permission before disclosing data to third parties, take appropriate precautions to protect data, and delete them when they are no longer required. 6. Leaders must ensure that staff members are trained in data-protection procedures and held accountable for following them by establishing protocols for identifying and responding to data-privacy breaches. 7. The aim of data-protection activities is to maintain a state of security and control risks throughout organizations by following organizational procedures and implementing technological solutions.	1. A lack of internal controls and employee factors can lead to data theft, highlighting the need for companies to implement and enforce effective data-protection practices. 2. Insufficient data-protection practices can harm a company's reputation and lead to legal and financial consequences. 3. Corporate-governance structures and stakeholder responsibility are crucial in creating a culture of data protection and ensuring accountability for data breaches. 4. Employees' awareness and understanding of data-protection policies and procedures are critical to the success of data-protection practices. 5. Ensuring data privacy and security is essential for building and maintaining strong customer relationships and trust, which are critical to the success of businesses in the current digital economy. 6. Leaders at all levels of an organization, not only risk-management and IT departments, are responsible for prioritizing data protection and taking proactive measures to minimize the risk of data breaches. 7. Companies need to have a thorough understanding of accountability and the role of auditors in ensuring compliance with data-protection regulations. 8. The management of risks in data protection requires ongoing education and training, as well as the continuous monitoring and evaluation of data-protection practices.	1. To ensure compliance with data-protection laws and regulations, companies should establish clear policies and procedures for managing and protecting data. 2. Companies can implement privacy-preserving machine-learning techniques to protect sensitive data while still allowing analysis and insights. 3. Regular reviews of and updates to data-protection policies, the performance of regular audits, and the provision of ongoing training to employees on data-protection practices can help ensure effective data protection. 4. Companies should establish procedures for detecting and addressing data-privacy breaches promptly, including incident-response plans and communication protocols. 5. The prioritization of employee responsibility and accountability, the careful recruitment of staff, the monitoring of customer data, oversight of third-party access, the use of advanced technology, the prevention of unauthorized access to data, and ensuring corporate governance structures and stakeholder responsibility for data protection are all important steps for effective data protection. 6. To build trust and address consumer-privacy concerns, online firms should adopt effective sales and marketing strategies that are transparent and respect customer-privacy preferences. 7. Leaders must obtain customers' consent before disclosing data to third parties, take necessary precautions to protect these data, and delete them when they are no longer required. They must also ensure that their employees are aware of and understand data-protection procedures and hold them accountable for following them.

6. Future Research Questions

This study shed light on the intersection of big data, AI, and privacy concerns in the fintech industry and proposed strategies for enhancing data protection and security. Nevertheless, to deepen our understanding of the ethical considerations in fintech, several themes demand further exploration. Future research could delve into the complex relationship between fintech and customer trust, with an emphasis on addressing data privacy and security concerns. Second, a study could be conducted to examine strategies for fostering trust in the fintech era, such as corporate digital responsibility or adherence to data-protection laws and regulations. Additionally, the impact of cultural and societal norms on the adoption of fintech and the use of big data and AI in the finance industry could be promising areas for future research. By exploring these themes, researchers can provide practical suggestions for stakeholders seeking to ensure the responsible and ethical use of big data and AI in the digital finance industry.

1. Ethical Considerations in Fintech: The Intersection of Big Data, AI, and Privacy
    - 1.1. What are the ethical implications of the integration of big-data analytics, artificial intelligence (AI), and financial technology (fintech) in the banking sector?
    - 1.2. How does the use of AI algorithms and big-data analytics in fintech raise concerns about privacy, fairness, transparency, bias, and the ownership and control of personal data?
    - 1.3. Which strategies and practices can fintech companies adopt to ensure the ethical use of customer data while harnessing the benefits of big data and AI?
2. Navigating the Complex Relationship between Fintech and Customer Trust: Addressing Data-Privacy and -Security Concerns
    - 2.1. How does customer trust in financial institutions influence the adoption and acceptance of fintech services, particularly regarding data privacy and security?
    - 2.2. What are the main concerns and vulnerabilities associated with data privacy and security in online banking, and how do they affect customer trust in fintech?
    - 2.3. Which measures can banks and financial-service providers implement to address data-security and -privacy concerns, enhance customer trust, and promote the broader adoption of fintech services?
3. Bridging the Trust Gap: Strategies for Fostering Trust in the Fintech Era
    - 3.1. How can organizations effectively implement corporate digital responsibility (CDR) practices to enhance financial performance and cultivate digital trust in the context of fintech?
    - 3.2. Which roles do transparency, integrity, reputation, and accountability play in fostering digital trust in fintech, and how can companies communicate these aspects through corporate reputation disclosures (CRDs)?
    - 3.3. What are the long-term benefits for organizations that adopt a culture of CDR and establish digital trust, and how can these benefits contribute to financial performance, brand equity, and marketability?
4. Ensuring Data Privacy and Security in the Digital Finance Industry: Best Practices and Strategies for Compliance with Data-Protection Laws and Regulations
    - 4.1. Which steps can financial institutions and fintech companies take to ensure compliance with data-protection laws and regulations, specifically concerning the General Data Protection Regulation (GDPR)?
    - 4.2. What are the best practices and strategies for protecting individuals' data in the digital finance industry, considering encryption, secure authentication protocols, de-identification techniques, data-governance frameworks, and regular audits?
    - 4.3. How can employee responsibility, accountability, and leadership practices contribute to data privacy and security within financial organizations, and

which measures can be taken to prevent data breaches and unauthorized access to customer data?

7. Conclusions

The integration of big data and AI in the fintech industry has created numerous benefits, including individualized financial services, increased operational efficiency, and cost reduction. However, this study revealed that addressing ethical and privacy concerns is crucial to maintaining customer trust and confidence. To this end, the study highlighted several best practices and approaches, such as responsible data collection and usage, reliable data-security measures, diverse and representative data sets, transparency, and compliance with data-protection laws and regulations. These findings have important policy implications. Firstly, policymakers should continue to monitor and adapt regulatory frameworks to keep pace with the evolving landscape of the fintech industry. This includes updating data-protection laws and regulations to address the challenges posed by big data and AI and ensuring that compliance and enforcement mechanisms are robust and effective. Collaborative efforts between fintech companies, regulators, and consumers are essential for addressing ethical and privacy challenges. Policymakers should foster dialogue and engagement among stakeholders to establish common standards, share best practices, and develop guidelines that encourage responsible data usage and protection.

Financial education is another policy implication that emerged from this study. Given the vulnerability of younger generations to the privacy risks associated with online banking, policymakers should prioritize financial education initiatives. By enhancing financial literacy and increasing awareness of data privacy and security among individuals, policymakers can empower consumers to make informed decisions and protect their personal information. Despite the valuable insights provided by this study, it is important to acknowledge its limitations. The selection of relevant studies may have influenced the scope and generalizability of the findings. The analysis is also limited by the availability and accessibility of data on specific fintech practices and their impact on ethical and privacy concerns.

Furthermore, the rapidly evolving nature of technology means that ethical and privacy considerations in the fintech industry are constantly changing, and the findings of this study may become outdated over time. Additionally, research bias may have been present despite efforts to ensure a comprehensive and systematic review process. The research team's choices and judgments throughout the review process may have introduced a certain level of subjectivity.

An awareness of these limitations is crucial for interpreting and applying the findings of this study. In conclusion, by considering the policy implications and limitations outlined above, policymakers, industry stakeholders, and researchers can work together to foster a responsible and ethically driven fintech ecosystem that prioritizes customer trust, data privacy, and societal well-being. Continued research and collaboration are needed to address emerging ethical and privacy concerns in the rapidly evolving fintech landscape and ensure the industry's sustainable growth.

Author Contributions: H.H.H.A.: supervision, project administration, funding, writing and editing. M.F.: conceptualization, data curation, data analysis, writing—original draft. All authors have read and agreed to the published version of the manuscript.

Funding: This research paper received funding from Dr. Hassan Aldboush who contributed financial support to the study. Dr. Hassan Aldboush had his contribution acknowledged in the funding of this study.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used in this literature review consisted of published articles, books, reports, and other scholarly sources that are publicly available. No primary data collection or generation was involved in this study. The literature sources were obtained from reputable academic databases, libraries, and online repositories. The specific citations and references for each source are provided in the reference section of this research paper, ensuring proper attribution to the original authors and publications.

Conflicts of Interest: The authors declare no conflict of interest related to this research. The study was conducted independently, and there were no financial or personal relationships that could have influenced the objectivity or integrity of the research. All data collection, analysis, and interpretation were carried out objectively and in accordance with ethical guidelines.

References

Abed, Ali Kamil, and Angesh Anupam. 2022. Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Security and Privacy* 6: e285. [CrossRef]

Abidin, Mohd Aizuddin Zainal, Anuar Nawawi, and Ahmad Saiful Azlin Puteh Salin. 2019. Customer data security and theft: A Malaysian organization's experience. *Information and Computer Security* 27: 81–100. [CrossRef]

Ashta, Arvind, and Heinz Herrmann. 2021. Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. *Strategic Change* 30: 211–22. [CrossRef]

Ayaburi, Emmanuel W. 2022. Understanding online information disclosure: Examination of data breach victimization experience effect. *Information Technology and People* 36: 95–114. [CrossRef]

Baumgartner, Kim T., Carolin A. Ernst, and Thomas M. Fischer. 2022. How Corporate Reputation Disclosures Affect Stakeholders' Behavioral Intentions: Mediating Mechanisms of Perceived Organizational Performance and Corporate Reputation. *Journal of Business Ethics* 175: 361–89. [CrossRef]

Beg, Saira, Saif Ur Rehman Khan, and Adeel Anjum. 2022. Data usage-based privacy and security issues in mobile app recommendation (MAR): A systematic literature review. *Library Hi Tech* 40: 725–49. [CrossRef]

Butaru, Florentin, Qingqing Chen, Brian Clark, Sanmay Das, Andrew W. Lo, and Akhtar Siddique. 2016. Risk and risk management in the credit card industry. *Journal of Banking and Finance* 72: 218–39. [CrossRef]

Castellanos Pfeiffer, Roberto Augusto. 2019. Digital economy, big data and competition law. *Market & Competition Law Review* 3: 53.

Daníelsson, Jón, Robert Macrae, and Andreas Uthemann. 2022. Artificial intelligence and systemic risk. *Journal of Banking and Finance* 140: 106290. [CrossRef]

Dixon-Woods, Mary. 2011. The role of qualitative research in systematic reviews. *Medical Education* 45: 332–38.

Erraissi, Allae, and Abdessamad Belangour. 2018. Data sources and ingestion big data layers: Meta-modeling of key concepts and features. *International Journal of Engineering & Technology* 7: 3607–12.

Fu, Jonathan, and Mrinal Mishra. 2022. Fintech in the time of COVID-19: Technological adoption during crises. *Journal of Financial Intermediation* 50: 100945. [CrossRef]

George, A. Shaji, and A. S. Hovan George. 2023. A review of ChatGPT AI's impact on several business sectors. *Partners Universal International Innovation Journal* 1: 9–23.

Goldstein, Itay, Wei Jiang, and G. Andrew Karolyi. 2019. To FinTech and beyond. *The Review of Financial Studies* 32: 1647–61.

Gong, Xiang, Kem ZK Zhang, Chongyang Chen, Christy M. K. Cheung, and Matthew K. O. Lee. 2020. What drives trust transfer from web to mobile payment services? The dual effects of perceived entitativity. *Information & Management* 57: 103250.

Herden, Christina J., Ervin Alliu, André Cakici, Thibaut Cormier, Catherine Deguelle, Sahil Gambhir, Caleb Griffiths, Shrishti Gupta, Sahil R. Kamani, Yonca-Selda Kiratli, and et al. 2021. Corporate Digital Responsibility. *Sustainability Management ForumNachhaltigkeitsManagementForum* 29: 13–29. [CrossRef]

Hermansyah, Muhammad, Ainun Najib, Any Farida, Rian Sacipto, and Bagus Setya Rintyarna. 2023. Artificial Intelligence and Ethics: Building an Artificial Intelligence System that Ensures Privacy and Social Justice. *International Journal of Science and Society* 5: 154–68. [CrossRef]

Jelovac, Dejan, Čedomir Ljubojević, and Ljubomir Ljubojević. 2021. HPC in business: The impact of corporate digital responsibility on building digital trust and responsible corporate digital governance. *Digital Policy, Regulation and Governance* 24: 485–97. [CrossRef]

La Torre, Matteo, Vida Lucia Botes, John Dumay, and Elza Odendaal. 2019. Protecting a new Achilles heel: The role of auditors within the practice of data protection. *Managerial Auditing Journal* 36: 218–39. [CrossRef]

Lacity, Mary C., and Leslie P. Willcocks. 2016. A new approach to automating services. *MIT Sloan Management Review* 58: 41–49.

Laksamana, Patria, Suharyanto Suharyanto, and Yohanes Ferry Cahaya. 2022. Determining factors of continuance intention in mobile payment: Fintech industry perspective. *Asia Pacific Journal of Marketing and Logistics*, *ahead-of-print*. [CrossRef]

Li, Jin, Ziwei Ye, and Caiming Zhang. 2022. Study on the interaction between big data and artificial intelligence. *Systems Research and Behavioral Science* 39: 641–48. [CrossRef]

Liyanaarachchi, Gajendra, Sameer Deshpande, and Scott Weaven. 2020. Market-oriented corporate digital responsibility to manage data vulnerability in online banking. *International Journal of Bank Marketing* 39: 571–91. [CrossRef]

Liyanaarachchi, Gajendra, Sameer Deshpande, and Scott Weaven. 2021. Online banking and privacy: Redesigning sales strategy through social exchange. *International Journal of Bank Marketing* 39: 955–83. [CrossRef]
Lobschat, Lara, Benjamin Mueller, Felix Eggers, Laura Brandimarte, Sarah Diefenbach, Mirja Kroschke, and Jochen Wirtz. 2021. Corporate digital responsibility. *Journal of Business Research* 122: 875–88. [CrossRef]
Lokanan, Mark E. 2014. How senior managers perpetuate accounting fraud? Lessons for fraud examiners from an instructional case. *Journal of Financial Crime* 21: 411–23. [CrossRef]
Malaquias, Rodrigo F., and Yujong Hwang. 2019. Mobile banking use: A comparative study with Brazilian and US participants. *International Journal of Information Management* 44: 132–40. [CrossRef]
Mars, Ammar, and Mohamed Salah Gouider. 2017. Big data analysis to features opinions extraction of customer. *Procedia Computer Science* 112: 906–16. [CrossRef]
Matzner, Tobias. 2014. Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data". *Journal of Information, Communication and Ethics in Society* 12: 93–106. [CrossRef]
Moscato, Donald R., and Shoshana Altschuller. 2012. International perceptions of online banking security concerns. *Communications of the IIMA* 12: 4. [CrossRef]
Peek, Sebastiaan T. M., Eveline J. M. Wouters, Joost Van Hoof, Katrien G. Luijkx, Hennie R. Boeije, and Hubertus J. M. Vrijhoef. 2014. Factors influencing acceptance of technology for aging in place: A systematic review. *International Journal of Medical Informatics* 83: 235–48. [CrossRef]
Saeidi, Sayedeh Parastoo, Saudah Sofian, Parvaneh Saeidi, Sayyedeh Parisa Saeidi, and Seyyed Alireza Saaeidi. 2015. How does corporate social responsibility contribute to firm financial performance? The mediating role of competitive advantage, reputation, and customer satisfaction. *Journal of Business Research* 68: 341–50. [CrossRef]
Saltz, Jeffrey S., and Neil Dewar. 2019. Data science ethical considerations: A systematic literature review and proposed project framework. *Ethics and Information Technology* 21: 197–208. [CrossRef]
Stewart, Harrison, and Jan Jürjens. 2018a. Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security* 26: 109–28. [CrossRef]
Stewart, Harrison, and Jan Jürjens. 2018b. Fintech and trust: A qualitative study of customers' attitudes towards fintech and their data protection concerns. *Journal of Financial Services Marketing* 23: 225–37.
Swammy, Sarah, Richard Thompson, Marvin Loh, Sarah Swammy, Richard Thompson, and Marvin Loh. 2018. A Vision for the Future: The Bermuda FinTech Story. *Crypto Uncovered* 173.
Vannucci, Virginia, and Eleonora Pantano. 2020. Do I Lose my Privacy for a Better Service? Investigating the Interplay between Big Data Analytics and Privacy Loss from Young Consumers' Perspective. In *Retail Futures*. Bingley: Emerald Publishing Limited, pp. 193–205. [CrossRef]
Yang, Jinlei, Yuanjun Zhao, Chunjia Han, Yanghui Liu, and Mu Yang. 2022. Big data, big challenges: Risk management of financial market in the digital economy. *Journal of Enterprise Information Management* 35: 1288–304. [CrossRef]
Yousafzai, Shumaila Y., John G. Pallister, and Gordon R. Foxall. 2005. Strategies for building and communicating trust in electronic banking: A field experiment. *Psychology & Marketing* 22: 181–201.
Yu, T. Robert, and Xuehu Song. 2021. Big Data and Artificial Intelligence in the Banking Industry. In *Handbook of Financial Econometrics, Mathematics, Statistics, and Machine Learning*. Singapore: World Scientific Publishing Co. Pte. Ltd., pp. 4025–41.