Journal of Islamic Economics Lariba
(P-ISSN 2477-4839 E-ISSN 2528-3758)
2023, Vol. 9, No. 2, 417-434
https://doi.org/10.20885/jielariba.vol9.iss2.art8

Customer data protection mitigations: Building Baitul Mal wa Tamwil transaction data security system in Lampung

Diana Ambarwati, & Hermanita

Program Studi Ekonomi Syariah (S1), Institut Agama Islam Negeri Metro, Metro, Indonesia

ABSTRAK

Introduction

Data security is a critical issue in today's digital age, exacerbated by the rampant online buying and selling of consumers' personal data. This study focuses on the strategies employed by microfinance institutions, specifically Baitul Maal wa Tamwil (BMT), to protect member data and manage the associated risks.

Objectives

The objective of this study is to describe mitigation strategies for data protection and risk management implemented by BMTs in Lampung.

Method

This field research employs qualitative methods, including observation and interviews, which are analyzed using the inductive thinking paradigm. Data collection focuses on BMTs' risk management practices and their cooperation with commercial banks to transfer risk.

Results

The findings reveal that BMTs in Lampung have implemented effective risk-management strategies for data protection. Some BMTs transfer risk to commercial banks, a strategy known as risk transfer. Others adopt risk reduction and acceptance strategies by enhancing data security, training employees on system use, and managing existing risks to minimize business impact.

Implications

This study highlights the importance of robust data protection and risk management strategies to maintain customer trust in microfinance institutions. Effective risk mitigation ensures customer data security, thereby enhancing the credibility and sustainability of BMTs.

Originality/Novelty

This study contributes to the understanding of data security practices in microfinance institutions, particularly in the context of Islamic microfinance, by exploring practical mitigation strategies and their implementation.

JEL Classification:
D82, G21, G32, L86, O16, Z12

KAUJIE Classification:
I67, L5, Q53

ARTICLE HISTORY:

Submitted: October 22, 2023
Revised: November 17, 2023
Accepted: November 22, 2023
Published: December 28, 2023

KEYWORDS:

Baitul Mal wa Tamwil; customer data; data protection mitigation; data security; security system; transaction data

Contact: Diana Ambarwati✉ dianaambarwati@metrouniv.ac.id

CITATION: Ambarwati, D. & Hermanita. (2023). Customer data protection mitigations: Building Baitul Mal wa Tamwil transaction data security system in Lampung. *Journal of Islamic Economics Lariba, 9*(2), 417-x. https://doi.org/10.20885/jielariba.vol9.iss2.art8

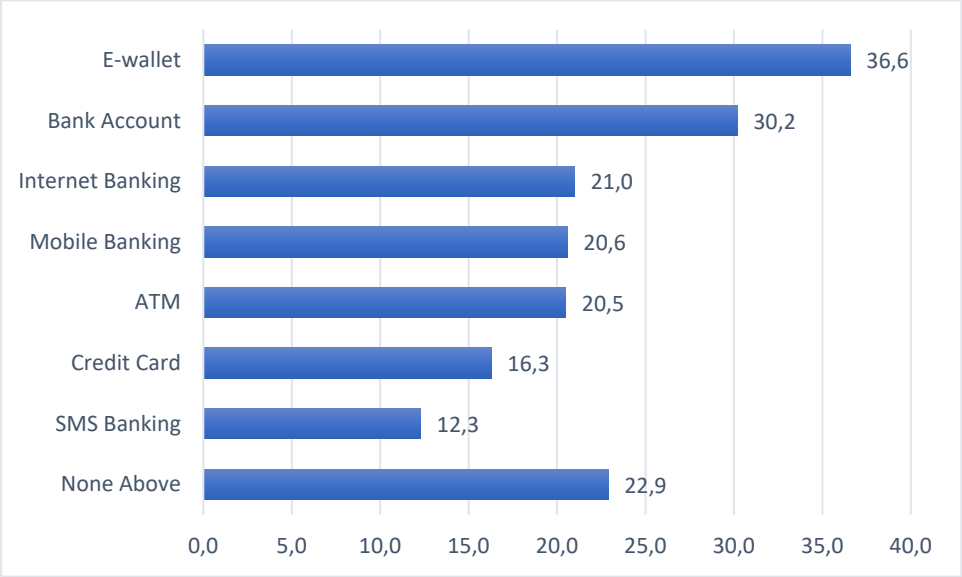
INTRODUCTION

The development of technology is something that its existence cannot touch. This technological development certainly greatly impacts all economic sectors, including the banking sector. The development of technology brings a breath of fresh air because it provides many uses, but the convenience offered also provides threats, especially personal data security. At least two cases have emerged; first, in mid-2020, Startexmislead accounts offered 12,957,573 records on the dark web Raid Forum; second, in mid-2021, Kotz account owners sold 279 million Indonesian population data on the same forum. Based on Cyber Patrol statistics, from January to December 2020 there were 2,259 reports from the public related to cybercrime (Bestari, 2021).

In the first quarter of 2022, detik.com reported that Indonesia was part of the top 10 countries that experienced data leakage cases. Even cyber Surfshark released data that Indonesia recorded 429.86 thousand users affected by data leakage cases. This phenomenon makes Indonesia the top country experiencing data leakage in Southeast Asia (Tim detikEdu, 2022). This phenomenon also afflicts financial institutions. Figure 1 explains Indonesian customers perception on banking products that are prone to data leakage including e-wallets, bank accounts, internet banking, mobile banking, bank ATMs, credit cards, and SMS banking (Mutia, 2022; Rizkinaswara, 2021).

Figure 1

Indonesian Customers Perception on Banking Products That are Prone to Data Leakage



Source: Kementerian Komunikasi dan Informatika (2021).

Based on the data in Figure 1, mobile banking occupies the fourth largest position experiencing data leakage. If converted to microfinance institutions, the development of logi technology is marked by the existence of mobile BMT (Baitul Mal wa Tamwil) or transaction facilities through devices. The presence of BMT mobile is an alternative media in the business of BMT microfinance institutions to pamper customers, where this is an effective solution to make transactions easily, quickly, anywhere and anytime (Berakon et al., 2021; Utama, 2021; Yunita, 2021). The use of mobile BMT in the microfinance institution industry is a significant breakthrough. Mobile BMT offers facilities that will provide benefits to customers and enable BMT to improve the quality of the services they provide.

Mobile BMT is different from conventional BMT services. In Mobile BMT, the invisible process raises many questions related to the legal regulation of customers' personal data (Hermansyah, 2000). Transactions in Mobile BMT not only involve BMT with customers, but involve many parties, including BMT, namely the internet service provider ,the merchant and the customer concerned (Riswandi, 2005).

This globalized and national phenomenon of consumer data security is a consequence of digitalization in all sectors. This is also experienced by micro and local entities. For example, as experienced by one of the BMT in Lampung who received a report from a customer stating that there was a hack of customer privacy data used in the BMT. This means that the phenomenon of data leakage is also experienced by small and micro financial management entities such as BMT. In this case, it is not yet known exactly what caused this personal data leak, whether there was a cyberattack, security system weaknesses or customer error or other things.

The experience of leaking customer privacy data security at BMT is interesting to discuss and find the root end. Maybe we think that customer data is safe in BMT. Given that BMT is a microfinance institution that serves small-scale financing, it is unlikely that cybercrime is interested in hacking. Or we can also think about what customer personal data will be used for, and so on. In fact, many scams with fake identities are in the name of someone to take financial advantage or to defame someone.

Based on this description of the incident, researchers want to know how the efforts made by micro sharia financial institutions in mitigating data security risks and controlling data leakage which will then result in customer distrust of these micro sharia financial institutions. This study is very interesting because it will contribute to the management of Islamic microfinance institutions, especially related to overcoming and anticipating leakage of customer privacy data security systems.

LITERATURE REVIEW

Research on data security until now is still seen from the point of normative law, has not touched on the sociological area that occurs in an entity. The studies that have been carried out are summarized in the following passages. Rumlus & Hartadi (2020) examined electronic information and transactions contained in Law No. 19 of 2016, and Government Regulation No. 71 of 2019 concerning the implementation of electronic systems and transactions, at the level of implementation is still ineffective and has not

guaranteed the security and protection of consumer personal data. Aswandi et al. (2020) found that regulation related to cybercrime is needed and also the protection of data and personal information in Indonesia. Furthermore, they suggest that a system is needed to enable to overcome cyber crime problems, especially in the field of data management and personal information, namely the Indonesian Data Protection System (IDPS).

Nurzie & Apriani (2021) discussed the responsibility of banks for leakage of confidential information, this article confirms that leakage of customer data generally involves insiders, both internal and affiliated parties who know the bank's security system. This means that there is an element of intentionality in the event of customer data leakage that occurs in banking. Saputra et al. (2022) found that effective cybersecurity will first and foremost secure customer data. Second, ethical behavior derived from Islamic beliefs will be able to prevent criminal activity and data breaches against consumers. Data privacy is a fundamental right that must be safeguarded collectively, according to Islam. Therefore, the key to fighting crime and misconduct in the digital environment is the precautionary principle of stakeholders.

Kusuma & Rahmani (2022) discussed data protection regulations that apply in Indonesia. The results of this study show that the enforcement of data hacking perpetrators has been regulated in Law number 36 of 1999 concerning telecommunications and Law number 7 of 1992 concerning banking with amendments to Law number 10 of 1998. This research also advises the government to immediately pass the Personal Data Protection Bill as a legal umbrella for personal data protection and can provide legal certainty for victims and considering Bank Indonesia's position as the central bank, Bank Indonesia's data security should be strictly maintained and controlled by related parties. This study recommends the immediate passage of consumer data protection laws so that perpetrators can be charged with crimes that create a deterrent. Karen governments have an obligation to protect the privacy data of their citizens. The legal perspective is very thick in this study, however, it has not yet addressed data security practices carried out by institutions such as banking or BMT.

Soemitra & Hasan (2022) explored how there are two means of legal protection, namely means of preventive legal protection and means of repressive legal protection. Means of preventive legal protection include regulation, guidance, socialization, complaint services, and sanctions. Meanwhile, repressive legal protection efforts are taken by litigation and non-litigation. Marcelliana et al. (2023) discussed how banking technology is getting more sophisticated with the use of features such as Internet Banking, ATM machines that are prone to abuse. Banking data leakage cases are behaviors that violate the principles of data security, data privacy, and ethics. The existence of a motive for data theft leads to loss of confidentiality, privacy, availability, and integrity of banking.

Dewata & Apriani (2023) discussed how the perspective of Law Number 7 of 1992 which was amended into Law Number 10 of 1998 concerning Banking, Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 8 of 1999 concerning Consumer Protection, Law Number 36 of 1999 concerning

Telecommunications sees customer data protection in dispute. The articles described above are very different from the research being conducted. Yustivasari's (2021) research is similar to this study in terms of customer data security in Sharia cooperatives. The limited studies discussing the incident of leakage and security of customer data at BMT could indicates less emphasize on BMT for its small size as institution. Thus, the data collected and managed is also small and the urgency is not significant. However, the fact that there is a leak of BMT customer data that occurs and raises the alarm that BMT is also being targeted by cyber criminals. This incident became the basis for researchers to try to explore more deeply how the customer data security system carried out by BMT. And this is what will be an important point of this study.

METHOD

This research is a field research that aims to understand the phenomena experienced by research subjects holistically, find value (*value-laden*), and not seek truth (Salim, 2001; Usman & Akbar, 2008) . The source of research data, primary data will be obtained directly from the object of research, namely the management and management of BMT in Lampung which has implemented a BMT mobile system with a different system typology, namely BMT atha Buana as a representative of USSI Group and BMT Asyafiiyyah Berkah Nasional as a representative of PT. Assist Software Indonesia Pratama. This research data collection method was carried out in three ways, namely observation, interviews and documentation. Observations were made by making observations on the Google PlayStore about the types and vendors of BMT mobile. This observation will find data on how the risk received by BMT with the use of this APK. And find the risk management used. In-depth interview (in-dept interview), to obtain information related to how to mitigate risks and also handle risks carried out by BMT to maintain customer data security. Documentation to obtain additional data sourced from relevant articles and journals. The final stage of this research is data processing and analysis using the inductive thinking paradigm.

RESULTS AND DISCUSSION

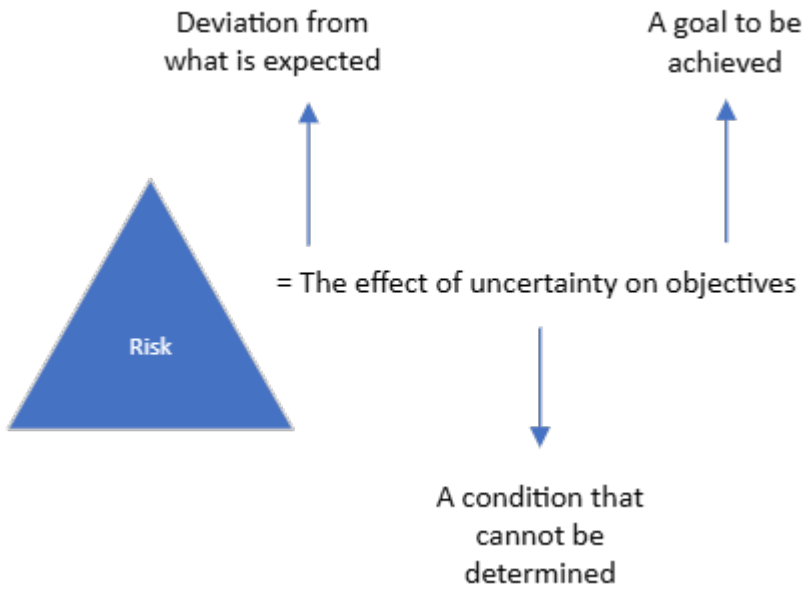
Risk Mitigation: A Conceptual Framework

Risk is the unpleasant or harmful effect of an action or action. Bank Indonesia defines risk as the potential loss due to the occurrence of a certain event. Risk is also defined as a form of uncertainty about a situation that will occur later (future) with decisions taken based on various considerations at this time (Fahmi, 2018). Another definition states that risk is uncertainty caused by changes in deviation from something expected (Jovanović, 2018). The international standard ISO 31000 (adopted by AS/NZS in AS/NZS ISO 31000:2009) defines risk as the effect of uncertainty on objectives (Lembaga Administrasi Negara, 2019). Risk is the probability of an outcome or *outcome* that is different from what is expected (Jamaluddin, 2018). Risk has characteristics, uncertainty

over the occurrence of an event and uncertainty which if it occurs will cause losses. In simple terms, risks can be described in Figure 2.

Figure 2

A Simple Overview of Risk



Source: Utari (2015).

Mitigation is linguistically defined as an action to reduce the impact of an event (Koc et al., 2021; Luna & Pennock, 2018). Thus, risk mitigation is identifying, evaluating, and reducing the possibility of adverse risks or impacts that can affect an organization, project, or activity (Handayani & Yusuf, 2022). The purpose of risk mitigation is to reduce adverse consequences if such risks occur, as well as to increase the likelihood of success or success of an initiative. Mitigation is ideally done by prior analysis based on some qualitative considerations. This is done so that the mitigation chosen is appropriate in dealing with risks, to minimize losses that may be caused. Some factors that need to be considered in determining mitigation activities well are: first, there is a cost-benefit analysis of mitigation of anticipated losses; second, do the mitigation timeline appropriately; third, the availability of resources (Firdaus, 2014).

In general, risk mitigation aims to reduce the possibility of risk occurrence and its impact on the business. There are several specific objectives of risk mitigation in a business context, among them improving security, improving reliability, increasing business resilience, and improving compliance (Hadi et al., 2020; Lutfi, 2011). There are some benefits of risk mitigation: first, minimize uncontrolled losses; second, give direction in seeing the influence that arises; third, encourage risk-averse decision-making; fourth, allocate capital and limit risk within the company; fifth, stakeholders are more careful in making decisions; and sixth, ensure that you do not experience unacceptable losses (Dermawi, 2016).

Risk management actions include: risk identification, identification of the likelihood of occurrence, identification of negative impacts generated, and thinking about how to overcome these risks or negative impacts. Actions against risk or risk impact can be classified into actions to avoid risk, deal with risk, and/or transfer the impact of risk (Green, 2016). The right type of risk mitigation should be based on the specific risks the business faces, available resources, and overall business objectives (Hanggraeni et al., 2019; Settembre-Blundo et al., 2021; Temel & Durst, 2020). In implementing appropriate risk mitigation strategies, businesses can reduce risk, protect business assets and reputation, and improve overall business success and continuity.

There are several types of risk mitigation that can be applied in a business context, namely risk avoidance, risk transfer, risk reduction, risk acceptance, and risk sharing (Fahmi, 2018). Furthermore, to solve risks is usually done in several ways such as mutual cooperation to map risks (risk mapping), mutual cooperation to provide solutions and choose the best alternative solution to be used as a recommendation, and mutual responsibility to resolve risks to completion (Herdiana et al., 2021).

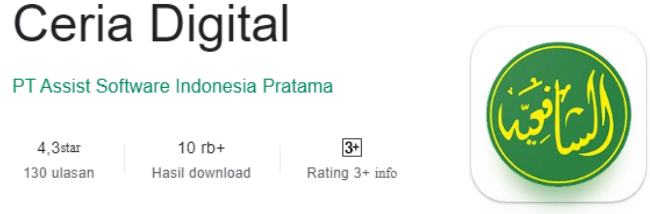
Use of Mobile Bmt in Sharia Microfinance Institutions

Baitul Maal wa Tamwil is a microfinance institution operated on the principle of profit sharing, growing and developing micro and small business businesses, in order to raise the status and character and defend the interests of the poor. This institution is a cooperative body. A cooperative according to Law No. 25 of 1992 is a business entity consisting of individuals or cooperative legal entities, by basing its activities on the cooperative principle as well as a people's economic movement based on kinship.

Baitul Maal Wa Tamwil Asyafiiyyah Berkah Nasional is a BMT that has been established since 1995, which has a vision of "to become a large, modern and quality cooperative". Currently, BMT Asyafiiyyah Berkah Nasional serves eleven savings products and six financing products. BMT Asyafiiyyah Berkah Nasional has a BMT mobile facility called ceria digital which has been implemented since February 2022. This application is the fruit of cooperation with PT. Assist Software Indonesia Pratama which is a vendor of many mobile BMT in Lampung. PT. Assist Software Indonesia Pratama is a company engaged in the field of Software Developer agency in charge of making responsive, safe, and quality Software. This company has collaborated with many BMTs in Lampung, one of which is BMT Asyafiiyyah Berkah Nasional.

Figure 3

Ceria Digital APK



Source: Google PlayStore.

This apk has been downloaded more than 10,000 times, 130 reviews, 4.3 stars and got a rating of 3+. The Ceria Digital application can be downloaded from Google PlayStore, with the display as in Figure 3.

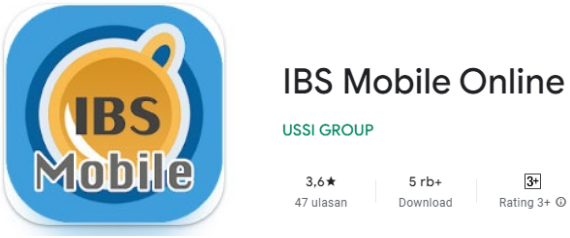
Just like mobile banking, Ceria Digital can serve various payments and financing from home without having to come to the office. As the following interview excerpt:

> "For Members who want to apply for financing, now there is no need to go to the nearest branch office. Simply through the online submission feature in the ceria digital application. Follow the steps, and then members will be surveyed by Marketing. For people who don't have a BMT account." (Personal communication)

Baitul Maal Wa Tamwil Arta has been established since 2013. The vision of BMT Artha Buana is "to become an independent, professional and trusted sharia microfinance institution", with the motto "rising together towards prosperity". IBS Mobile Online by BMT Artha Buana is the result of collaboration between BMT Artha Buana, Bank Muamalat Indonesia and USSI group. IBS Syariah used by BMT Artha Buana is an APK used by Bank Muamalat Indonesia. BMT Artha Buana uses IBS mobile online as an extension of Muamalat bank. This means that every BMT Artha Buana and all its members have an account at Bank Muamalat. This apk has been downloaded 5,000 times, received 47 reviews, 3.6 stars and a rating rating of 3+. The display of IBS mobile online on PlayStore is as in Figure 4.

Figure 4

IBS Mobile Online APK



Source: Google PlayStore.

Risk Mitigation Model in Mobile BMT Type Selection

Risk mitigation is the process of identifying, evaluating, and reducing the likelihood of negative risks or impacts that may affect an organization, project, or activity. The purpose of risk mitigation is to reduce adverse consequences if such risks occur, as well as to increase the likelihood of success or success of an initiative.

It is important to remember that risk mitigation cannot eliminate risk as a whole but rather aim to reduce it as far as possible. Risk mitigation efforts should be based on careful assessment and carried out on an ongoing basis to maintain the success and sustainability of an activity or initiative.

On the BMT mobile usage context, BMT has performed the identification of the advantages and disadvantages of the BMT mobile to be used. consideration of the convenience and similarity of the system. This makes BMT Artha Buana choose mobile

BMT in collaboration with Bank Muamalat Indonesia, compared to making mobile BMT independently. In addition to the consideration of system similarity, BMT Artha Buana views that if you make it independently, it will cost a high investment cost and it will put a burden on BMT to recover its investment costs. In addition, some features are difficult to access, for example transfers to other banks.

BMT Artha Buana also considered the possibilities of cooperation related to BMT's mobile. This shows that BMT has analyzed the capabilities and opportunities in selecting the type of cooperation related to this BMT mobile. However, there are weaknesses in taking this stance. Because BMT Artha Buana is BMI's partner, BMT Artha Buana only follows the features provided by Bank Muamalat. BMT Artha Buana cannot develop features independently. Although the resource person stated that the IBS mobile feature owned by Bank Muamalat is representative enough to make it easier for customers to make transactions.

Then when asked about the risk of data leakage that might occur a over the use of this BMT mobile, the source stated that if there is a data leak it is the responsibility of the owner of the BMT mobile APK in this case Bank Muamalat. BMT Artha Buana, which incidentally, as a customer, can sue for the data leak. If it is related to the concept of risk, the attitude and actions of BMT Artha Buana who choose to cooperate with Bank Muamalat in order to transfer risk (risk transfer), which means BMT Artha Buana involves and transfers risk to other parties, in this case Bank Muamalat Indonesia. Risk transfer is a strategy or action taken to reduce or transfer potential losses or risks from one party to another (Khan & Sarkar, 2021). This act of risk transfer does not always mean eliminating the risk completely. It simply reduces the potential impact of the risk or transfers the risk to another party who is better able to manage it (Sigalingging et al., 2022).

What is described above, namely the action of selecting *risk transfer* carried out by BMT Artha Buana, is different from BMT Asyafiiyyah Berkah Nasional, which has a mobile BMT independently and directly cooperates with the current party, namely PT. Assist Software Indonesia Pratama as a BMT mobile service provider, which was later named Ceria Digital. BMT Asyafiiyyah plans the process of selecting vendors or partners through careful planning and analysis. Vendor selection decision makers. This process also takes a long time. This certainly implies a fairly tough tug-of-war between the executor and the BMT management. Tug of war between the benefits that will be obtained and the risks that may be faced. In addition, BMT also sees and considers the financial capabilities and the feasibility of the investment to be made.

If examined carefully, it appears that there is careful planning and consideration to finally invest funds for the procurement of this BMT mobile. Conceptually this step is a form of risk mitigation that aims to reduce the possibility of an information failure, and several other parts to work to reduce the amount of loss caused by that failure. The control function ensures that whatever form the threat manifests, there is one or more opportunities for controls to mitigate the risk (Nuriah et al., 2021).

This attitude is actually based on the fact that the use of mobile BMT provides many benefits for both managers and mobile BMT users, in this case members. *First*, ease of

access, as research conducted by Khtufia et al. (2022) stating that IBS Mobile provides easy access to access account anytime and anywhere using your mobile device. This provides greater flexibility and eliminates the time and place limitations typically associated with financial transactions. *Second,* time efficiency since through BMT mobile, BMT customers can make transactions quickly and easily. They can check account balances, transfer funds, pay bills, and view transaction history without having to come to the BMT office. This can save time and effort in managing their finances (Nuriah et al., 2021).

Third, security since Mobile BMT is generally equipped with advanced security technologies, such as two-factor authentication, data encryption, and protection via PIN or fingerprint. This helps maintain customer privacy and security when conducting financial transactions through the BMT mobile application (Bakhri et al., 2022). *Fourth,* notifications and Notifications: BMT mobile apps often provide notification and notification features. Customers will receive immediate notifications about transactions, account balances, or other important changes. This helps customers stay up-to-date with their financial activities and allows quick responses in case of unusual events (Jannah et al., 2023).

Fifth, Additional Services: In addition to basic functions such as transfers and payments, mobile banking on BMT also often provides additional services such as credit purchases, bill payments, ticket purchases, and others (Jannah et al., 2023). This provides convenience for customers in accessing various financial services in one application (Bakhri et al., 2022). *Sixth,* Better Financial Management. With easy access to their financial information through the BMT mobile application, BMT customers can better monitor and manage their finances (Bakhri et al., 2022).

Furthermore, related to the selection of mobile BMT that does not involve parties other than BMT and Vendors, the risk will likely be the direct responsibility of BMT and Vendors. Aware of the risks involved, BMT sent a team to learn about the system. This step means that BMT Asyafiiyyah is carrying out a *Risk Reduction* strategy. This risk mitigation strategy involves actions to reduce the likelihood or impact of emerging risks. This can be done in various ways, such as improving security procedures, making technological improvements, improving employee training, or improving operational processes. The purpose of this strategy is to reduce existing risks and minimize the possibility of losses or adverse dampak on the business.

In addition, BMT Asyafiiyyah is carrying out a *Risk Acceptance* strategy, which is a mitigation step by deciding to accept existing risks and manage them in a way that can minimize their impact on the business. Risk acceptance is used when the cost or resources required to mitigate risk are too high and the likelihood of risk occurring is relatively low (Fahmi, 2018).

Customer Data Security Protection Mitigation

Digital economy, which is currently being promoted by every stakeholder, both government and private, with the slogan "everything is digital," provides a lot of extra convenience and comfort. However, personal data security threats are also following

these developments. Personal data, which is a human right, has been widely recognized. In business, protecting consumers' personal data is an important part of safeguarding the privacy of individuals and their rights. Institutions have a moral responsibility to respect consumer privacy and prevent misuse or unauthorized access to their personal data.

Thus, the behavior of leaking data or stealing someone's personal data is a violation of human rights (Soraja, 2021). This behavior also violates the law on consumer personal data protection. Each institution is obliged to comply with this regulation and protect consumers' personal data in accordance with applicable legal requirements. Violation of these regulations may result in legal sanctions and a bad reputation for the institution.

If a data leak occurs, it will have a serious impact on the company, not only can it result in financial losses, damaged reputation, and even lawsuits, but data leakage will have an impact on the possibility of misuse of data by other parties. Therefore, mitigating the risk of data leakage is an important thing that must be done by companies, including BMT. BMT is one of the entities that collects customer personal data for financial transaction purposes. In this study, BMT management will be prepared to anticipate customer data leakage, especially data leakage caused by the use of BMT mobile, both policy preparedness, commitment, anticipation efforts and handling efforts. Based on the results of the study, facts and data were found about mitigating the risk of BMT data leakage in Lampung, as follows:

Data Protection and Security Policy in BMT

A data protection and security policy is a document that describes how an organization will collect, manage, protect, and use the personal data of customers, employees, or other parties associated with that organization. This policy is important to ensure that sensitive data is not misused or exposed by unauthorized parties (Saleh, 2021).

In this regard, BMT leaders stated that they do not yet have a document that specifically regulates how to protect and secure customer data, but in practice the SOP applied guarantees that data will not be misused. The two BMTs studied have not compiled and have specific documents related to personal data protection, however, in the process of serving, BMT realizes that Personal Data is data that is a bank secret which is a priority for protection. So all BMT employees must be given training related to data security and how to recognize potential threats. They should also know how and how to report security incidents.

Several institutions, both government and private, such as BPJS, have currently implemented ISO 27001 (certified) standard data security systems, *Control Objectives for Information Technologies* (COBIT) and operate a *Security Operation Center* (SOC) that works 24 hours 7 days. In addition, BPJS also collaborates with the National Cyber and Encryption Agency (BSSN) to uncover data breaches in BPJS Kesehatan (Saleh, 2021). If deemed necessary, BMT can follow this step, namely collaborating and involving other parties to help secure the personal data of its members. Thus, members feel safe and comfortable in transacting. Of course, this will increase public trust or trust to maximize transactions using mobile BMT.

Currently, many good government companies use big data to protect consumers' data. The challenge today is more related to how companies optimize their data. Regarding privacy violations, there needs to be legal certainty and understanding of ethics in the use of information technology (Pujianto et al., 2018). BMT recommends two-factor authentication, which customers use when accessing their accounts. This adds another layer of security by requiring something they know (a password) and something they have (for example, a code sent via SMS).

BMT's Commitment to Maintaining Data Privacy as an Effort to Maintain Customer Trust

Financial Institutions that play a role in managing customer data have an obligation to maintain the confidentiality and security of customer data (Bakhri et al., 2022). This is because there are several important reasons related to the privacy and security of personal information. Personal data is a human right which then becomes the obligation of every institution that manages personal data to safeguard it (Pujianto et al., 2018).

In addition, data insecurity can lead to financial misuse, fraud, or identity theft. When institutions maintain data security, it has indirectly helped protect customers from adverse financial risks. BMT as an institution also has the obligation to safeguard basic personal data when transacting.

When transacting, each customer will provide personal information to microfinance institutions, in this case BMT, with the hope that in addition to getting services according to customer needs, they believe that the data they provide will be secured and protected as appropriate. If BMT does not maintain the security of the data, this results in damage to customer trust and also the integrity of the institution is questioned. Customer trust is the key to BMT's sustainability.

BMT is committed to safeguarding the personal data of its customers. Not only owned by the leader but also employees have the same commitment in this regard. Commitment to BMT stakeholders is important to safeguard customers' personal data. Commitment is a form of responsibility by BMT for customer personal data.

This is done in order to maintain customer trust. In the digital era, customer data protection is very important. Businesses that ensure the security of customers' personal data and maintain their privacy will build strong trust. Trust is a valuable asset in the financial business. It takes time and consistent effort to maintain. BMT protects customer data as a form of implementation of the mandate of Law Number 22 of 2022 concerning consumer data protection. In this case, BMT is the data manager. In addition, the mandate of the applicable law requires companies to maintain the confidentiality and privacy of customer data. This must be done by collecting data only from legitimate sources, using customer data only for specified purposes, and not divulging customer data to other parties without the consent of the customer.

In addition, BMT must also ensure customer data security through adequate security technology, such as data encryption, firewalls, antivirus, and other network security technologies. BMT must also monitor customer data usage activities to prevent unauthorized access and data security breaches.

When viewed from the IBS Mobile online app owned by USSI Group, the data security description states that the developer does not collect or share user data with other companies and organizations.

Mitigating the risk of consumer data leakage is critical to protecting personal and sensitive data from unauthorized access or unwanted disclosure. In this increasingly advanced digital era, consumer data protection is necessary for companies and organizations that collect and store such data.

This means that consumer data leakage in BMT is a serious problem that must be taken seriously by the institution. Consumer data protection is BMT's main responsibility, as well as maintaining consumer trust and complying with applicable regulations. Awareness of the risk of consumer data leakage is an important first step. BMTs must be aware of the potential threats and repercussions that may occur if their consumer data falls into the wrong hands.

The steps taken by BMT Artha Buana who chose to cooperate with Bank Muamalat Indonesia and USSI Group. The BMT mobile application used belongs to Bank Muamalat Indonesia and USSI Group. BMT is only a customer of BMI and USSI Group. The application owner, namely BMI, owns the risk of customer data leakage through the application. This collaboration is quite effective, where BMT does not have direct responsibility for the risk of data leakage that may be experienced due to the use of IBS mobile online. Risk transfer and sharing are steps taken by BMT Artha Buana to minimize the risk of data leakage.

Risk transfer is a risk mitigation strategy that involves transferring risk to other parties, in this case BMI and USSI Group. Simply by providing an administration fee of Rp. 2,000, - to BMI, all BMT Artha members can enjoy the convenience of transactions without restrictions. BMI and USSI can be ensured to have sufficient financial capacity and expertise to mitigate the risks transferred to them. BMT Artha believes that BMI and USSI have a safe and secure information technology infrastructure from cyber-attacks and threats. It involves the use of firewalls, intrusion detection systems, network monitoring, and other security measures to prevent unauthorized access.

The use of Ceria Digital by BMT Asyafiiyyah in collaboration with PT. Assist is a step and breakthrough to facilitate transactions. In terms of the risk of leakage of customers' data, this form of mobile BMT is quite risky and BMT Asyafiiyyah takes this risk. Anticipatory steps taken by BMT so that the risk of data leakage can be minimized by reducing the use of Ceria Digital related to outside parties such as transfers to other banks, because it is considered the most potential for data leakage. If this happens, then it is likely to have cost consequences if you want to fix the app soon. So, the step is to limit the use of digital cherries for needs related to transfers to other banks.

CONCLUSION

Based on the explanation in the previous chapter, it can be concluded several things, namely that BMT Artha Buana chose to cooperate with Bank Muamalat to transfer risk (*Risk Transfer*), which means BMT Artha Buana involves and transfers risk to other parties in this case Bank Muamalat Indonesia. Risk transfer is a strategy or action taken

to reduce or transfer potential losses or risks from one party to another. Meanwhile, BMT Asyafiiyyah alternately carries out Risk Reduction and Risk Acceptance strategies by preparing data security, sending employees to learn about the systems used, and ultimately deciding to accept the existing risks and manage them in a way that can minimize their impact on the business.

Ensuring the security of customer data is one key to maintaining customer trust in financial institutions. This trust-based business is highly dependent on trust. The destruction of trust means the destruction of institutions. Customers place great trust in financial institutions to protect their personal information, including financial and identity data. If a financial institution is unable to keep this data secure, customers can lose trust in the institution, which can result in loss of business.

Author Contributions

Conceptualization	D.A. & H.	Resources	D.A. & H.
Data curation	D.A. & H.	Software	D.A. & H.
Formal analysis	D.A. & H.	Supervision	D.A. & H.
Funding acquisition	D.A. & H.	Validation	D.A. & H.
Investigation	D.A. & H.	Visualization	D.A. & H.
Methodology	D.A. & H.	Writing – original draft	D.A. & H.
Project administration	D.A. & H.	Writing – review & editing	D.A. & H.

All authors have read and agreed to the published version of the manuscript.

Funding

This study received no funding from any institution.

Institutional Review Board Statement

The study was approved by Program Studi Ekonomi Syariah (S1), Institut Agama Islam Negeri Metro, Metro, Indonesia.

Informed Consent Statement

Informed consent was obtained before respondents answered the questions.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Acknowledgments

The authors thank Program Studi Ekonomi Syariah (S1), Institut Agama Islam Negeri Metro, Metro, Indonesia, for administrative support for the research on which this article was based.

Conflicts of Interest

The authors declare no conflicts of interest.

REFERENCES

Aswandi, R., Muchin, P. R. N., & Sultan, M. (2020). Perlindungan data dan informasi pribadi melalui Indonesian Data Protection System (IDPS) [Protection of data and personal information through the Indonesian Data Protection System (IDPS)]. *Jurnal Legislatif*, *3*(2), 167–190. https://doi.org/10.20956/jl.v3i2.14321

Bakhri, S., Rofiq, A., & Faizun, D. (2022). Analisis faktor – faktor penggunaan aplikasi mobile dalam meningkatkan jasa layanan terhadap lembaga keuangan mikro syariah [Analysis of factors for the use of mobile applications in improving services to Islamic microfinance institutions]. *Tasharruf*: *Journal of Islamic Economics and Business*, *3*(2), 73–87. https://doi.org/10.55757/tasharruf.v3i2.208

Berakon, I., Aji, H. M., & Hafizi, M. R. (2021). Impact of digital Sharia banking systems on cash-waqf among Indonesian Muslim youth. *Journal of Islamic Marketing*, *13*(7), 1551–1573. https://doi.org/10.1108/JIMA-11-2020-0337

Bestari, N. P. (2021, September 7). *Banyak data pribadi dijual di Dark Web, Harganya bikin kaget [A lot of personal data is sold on the Dark Web, the price is shocking]* [HTML]. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20210907115829-37-274255/banyak-data-pribadi-dijual-di-dark-web-harganya-bikin-kaget

Dermawi, H. (2016). *Manajemen risiko [Risk management]*. Bumi Aksara.

Dewata, Y. J., & Apriani, R. (2023). Legal protection against internet banking users (mobile banking) from cyber crime efforts. *Soedirman Law Review*, *5*(1), 1–13. https://doi.org/10.20884/1.slr.2023.5.1.79

Fahmi, I. (2018). *Manajemen risiko, teori & solusi [Risk management, theory & solutions]*. Alfabeta.

Firdaus, Z. A. (2014). *Mitigasi risiko pembiayaan di lembaga keuangan mikro Islam [Mitigating financing risks in Islamic microfinance institutions]* [M.A. Thesis, Universitas Airlangga]. http://lib.unair.ac.id

Green, P. E. J. (2016). Introduction to risk management principles. In *Enterprise risk management* (pp. 1–13). Elsevier. https://doi.org/10.1016/B978-0-12-800633-7.00001-8

Hadi, J. A., Febrianti, M. A., Yudhistira, G. A., & Qurtubi, Q. (2020). Identifikasi risiko rantai pasok dengan metode house of risk (HOR) [Identification of supply chain risks with the house of risk (HOR) method]. *Performa*: *Media Ilmiah Teknik Industri*, *19*(2), 85–94. https://doi.org/10.20961/performa.19.2.46388

Handayani, W., & Yusuf, M. A. (2022). Analisis dan mitigasi resiko rantai pasok dengan metode AHP dan FMEA [Analysis and mitigation of supply chain risks with AHP and FMEA methods]. *Revitalisasi*, *11*(1), 43. https://doi.org/10.32503/revitalisasi.v11i1.2501

Hanggraeni, D., Ślusarczyk, B., Sulung, L. A. K., & Subroto, A. (2019). The impact of internal, external and enterprise risk management on the performance of micro, small and medium enterprises. *Sustainability*, *11*(7), Article 7. https://doi.org/10.3390/su11072172

Herdiana, Y., Munawar, Z., & Indah Putri, N. (2021). Mitigasi ancaman resiko keamanan siber di masa pandemi COVID-19 [Mitigating cybersecurity risks during the COVID-19 pandemic]. *Jurnal ICT*: *Information Communication & Technology*, *20*(1), 42–52. https://doi.org/10.36054/jict-ikmi.v20i1.305

Hermansyah. (2000). *Hukum perbankan nasional Indonesia [Indonesian national banking law]*. Kencana Prenada Media Group.

Jamaluddin, F. (2018). Mitigasi resiko kredit perbankan [Bank credit risk mitigation]. *Al-Amwal*: *Journal of Islamic Economic Law*, *3*(1), 83–95. https://doi.org/10.24256/alw.v3i1.201

Jannah, N. K., Husainah, R. A., & Ma'shum, A. H. (2023). Analisis minat nasabah dalam penggunaan layanan mobile banking pada KSPPS BMT Bahtera Pekalongan [Analysis of customer interest in using mobile banking services at KSPPS BMT Bahtera Pekalongan]. *Jurnal BANSI - Jurnal Bisnis Manajemen Akutansi*, *2*(2), 55–66. https://doi.org/10.58794/bns.v2i2.69

Jovanović, Z. M. (2018). Risk management in banking. *Zbornik Radova Pravnog Fakulteta u Nišu*, *57*(81), 139–150. https://doi.org/10.5937/zrpfni1881139J

Kementerian Komunikasi dan Informatika. (2021). *Persepsi Masyarakat atas Pelindungan Data Pribadi: Survei Nasional Tahun 2021 [Public Perception on Personal Data Protection: 2021 National Survey]*. Kementerian Komunikasi dan Informatika.

Khan, I., & Sarkar, B. (2021). Transfer of risk in supply chain management with joint pricing and inventory decision considering shortages. *Mathematics*, *9*(6), 638. https://doi.org/10.3390/math9060638

Khtufia, M., Novian, H. N., & Hidayah, A. F. H. (2022). Peran pelayanan aplikasi IBS Mobile dalam meningkatkan kepuasan anggota KSPPS BMT Artha Buana Metro Lampung [The role of IBS Mobile application services in increasing member satisfaction KSPPS BMT Artha Buana Metro Lampung]. *Falah Journal of Sharia Economic Law*, *3*(2), 87–94. https://doi.org/10.55510/fjhes.v3i2.150

Koc, K., Ekmekcioğlu, Ö., & Özger, M. (2021). An integrated framework for the comprehensive evaluation of low impact development strategies. *Journal of Environmental Management*, *294*, 113023. https://doi.org/10.1016/j.jenvman.2021.113023

Kusuma, A. C., & Rahmani, A. D. (2022). Analisis yuridis kebocoran data pada sistem perbankan di Indonesia (Studi kasus kebocoran data pada Bank Indonesia) [Juridical analysis of data leakage in the banking system in Indonesia (Case study of data leakage at Bank Indonesia)]. *Supremasi: Jurnal Hukum*, *5*(1), 46–63. https://doi.org/10.36441/supremasi.v5i1.721

Lembaga Administrasi Negara. (2019). *Modul manajemen risiko pelatihan kepemimpinan administrator [Administrator leadership training risk management module]*. Lembaga Administrasi Negara.

Luna, S., & Pennock, M. J. (2018). Social media applications and emergency management: A literature review and research agenda. *International Journal of Disaster Risk Reduction*, *28*, 565–577. https://doi.org/10.1016/j.ijdrr.2018.01.006

Lutfi, A. (2011). *Analisis risiko rantai pasok dengan model house of risk (HOR) [Supply chain risk analysis with the house of risk (HOR) model]* [Bachelor's thesis, Universitas Telkom]. https://repository.telkomuniversity.ac.id/pustaka/14328/analisis-risiko-rantai-pasok-dengan-model-house-of-risk-hor-.html

Marcelliana, V., Zahra, S. M., Adzani, N. N., Massaid, H. N., Badriyyah, N., Benita, R., Sukarto, M., Fitriani, C. N., & Bayhaqi, T. A. R. (2023). Penerapan perlindungan konsumen terhadap nasabah PT. Bank Syariah Indonesia dalam kasus kebocoran data nasabah [Implementation of consumer protection for customers of PT Bank Syariah Indonesia in the case of customer data leakage]. *Deposisi: Jurnal Publikasi Ilmu Hukum*, *1*(2), 180–194. https://doi.org/10.59581/deposisi.v1i2.577

Mutia, A. (2022, October 14). *Survei: Ini produk keuangan yang dianggap rentan kebocoran data [Survey: These are the financial products considered vulnerable to data leakage]* [HTML]. Databoks. https://databoks.katadata.co.id/layanan-konsumen-kesehatan/statistik/9e47e8a7538de5d/survei-ini-produk-keuangan-yang-dianggap-rentan-kebocoran-data

Nuriah, S., Rois, B., & Risnaeni, U. S. (2021). Efektivitas manajemen risiko dan hasil [Risk management effectiveness and results]. *Muhasabatuna: Jurnal Akuntansi Syariah*, *1*(2), 1. https://doi.org/10.54471/muhasabatuna.v1i2.1262

Nurzie, F., & Apriani, R. (2021). Tanggung jawab perbankan terhadap nasabah atas kebocoran informasi pribadi nasabah bank [Liability of banks to customers for leakage of personal

information of bank customers]. *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat*, *7*(2), 227–234. https://doi.org/10.55809/tora.v7i2.6

Pujianto, A., Mulyati, A., & Novaria, R. (2018). Pemanfaatan big data dan perlindungan privasi konsumen di era ekonomi digital [Utilization of big data and consumer privacy protection in the digital economy era]. *Majalah Ilmiah Bijak*, *15*(2), 127–137. https://doi.org/10.31334/bijak.v15i2.201

Riswandi, B. A. (2005). *Aspek hukum internet banking [Legal aspects of internet banking]*. PT Raja Grafindo.

Rizkinaswara, L. (2021, December 9). Kominfo lakukan survei nasional untuk gali persepsi masyarakat dan kesiapan industri atas penerapan PDP [Kominfo conducts national survey to explore public perception and industry readiness for PDP implementation] [HTML]. *Ditjen Aptika*. https://aptika.kominfo.go.id/2021/12/kominfo-lakukan-survei-nasional-untuk-gali-persepsi-masyarakat-dan-kesiapan-industri-atas-penerapan-pdp/

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik [Policy on countermeasures against theft of personal data in electronic media]. *Jurnal HAM*, *11*(2), 285. https://doi.org/10.30641/ham.2020.11.285-299

Saleh, Abd. R. (2021). Perlindungan data pribadi dalam perspektif kebijakan hukum pidana [Personal data protection in the perspective of criminal law policy]. *HUKMY : Jurnal Hukum*, *1*(1), 91–108. https://doi.org/10.35316/hukmy.2021.v1i1.91-108

Salim, A. (2001). *Teori dan paradigma penelitian sosial [Social research theories and paradigms]*. Tiara Wacana.

Saputra, A. A., Fasa, M. I., & Ambarwati, D. (2022). Islamic-based digital ethics: The phenomenon of online consumer data security. *Share: Jurnal Ekonomi Dan Keuangan Islam*, *11*(1), 105–128. https://doi.org/10.22373/share.v11i1.11167

Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S., & García-Muiña, F. E. (2021). Flexibility and resilience in corporate decision making: A new sustainability-based risk management system in uncertain times. *Global Journal of Flexible Systems Management*, *22*(2), 107–132. https://doi.org/10.1007/s40171-021-00277-7

Sigalingging, O. P. S., Sagala, M. J. P., & Gultom, M. (2022). Perlindungan hukum bagi pemegang polis dari perusahaan asuransi jiwa yang pailit [Legal protection for policyholders of bankrupt life insurance companies]. *Jurnal Impresi Indonesia*, *1*(7), 773–785. https://doi.org/10.58344/jii.v1i7.206

Soemitra, A., & Hasan, A. (2022). Perlindungan konsumen terhadap kebocoran data pada jasa keuangan di Indonesia [Consumer protection against data leaks in financial services in Indonesia]. *Juripol (Jurnal Institusi Politeknik Ganesha Medan)*, *5*(1), 288–303. https://jurnal.polgan.ac.id/index.php/juripol/article/view/11538

Soraja, A. (2021). Perlindungan hukum atas hak privasi dan data pribadi dalam prespektif HAM [Legal protection of privacy rights and personal data in human rights perspective]. *Seminar Nasional - Kota Ramah Hak Asasi Manusia*, *1*, 20–32. https://conference.untag-sby.ac.id/index.php/semnas/article/view/168

Temel, S., & Durst, S. (2020). Knowledge risk prevention strategies for handling new technological innovations in small businesses. *VINE Journal of Information and Knowledge Management Systems*, *51*(4), 655–673. https://doi.org/10.1108/VJIKMS-10-2019-0155

Tim detikEdu. (2022, September 16). *Indonesia masuk 10 besar negara kasus kebocoran data terbanyak [Indonesia is among the top 10 countries with the most data leakage cases]* [HTML].

Detikbali. https://www.detik.com/bali/berita/d-6295679/indonesia-masuk-10-besar-negara-kasus-kebocoran-data-terbanyak

Usman, H., & Akbar, P. S. (2008). *Metodologi penelitian sosial [Social research methodology]*. Bumi Aksara.

Utama, A. S. (2021). Digitalisasi produk bank konvensional dan bank syariah di Indonesia [Digitalization of conventional and Islamic bank products in Indonesia]. *Jurnal Justisia*: *Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial*, *6*(2), 113–126. https://doi.org/10.22373/justisia.v6i2.11532

Utari, R. (2015). *Perancangan strategi mitigasi resiko supply chain di PT Atlas Copco Nusantara dengan metoda house of risk [Designing supply chain risk mitigation strategies at PT Atlas Copco Nusantara with the house of risk method]* [Bachelor's thesis, Institut Teknologi Sepuluh Nopember]. https://repository.its.ac.id/1079/

Yunita, P. (2021). The digital banking profitability challenges: Are they different between conventional and Islamic banks? *Jurnal Akuntansi Dan Keuangan Indonesia*, *18*(1), 55–74. https://doi.org/10.21002/jaki.2021.04

Yustivasari, A. (2021). *Penerapan algoritma Base64 pada sistem koperasi syariah guna meningkatkan keamanan data nasabah [Application of Base64 algorithm in sharia cooperative system to improve customer data security]* [Bachelor's thesis, Universitas Muhammadiyah Ponorogo]. http://eprints.umpo.ac.id/7283/