Inovbiz: Jurnal Inovasi Bisnis 12 (2024) 200-206
INOVBIZ
Website: www.ejournal.polbeng.ac.id/index.php/IBP
Email: inovbiz@polbeng.ac.id

Digital Financial Transactions Using QRIS Reviewed From The Legal Aspects

Benny Cuaca[1], Fridayani[2]

[1] Universitas Pelita Harapan Surabaya, Surabaya. Indonesia, bennycuaca@yahoo.com
[2] Universitas Pamulang, Banten, Ineodnesia, dosen02918@unpam.ac.id

ARTICLE INFO

Received: (April 19, 2024)
Received in revised: (September 16, 2024)
Accepted: (December 10, 2024)
Published: (December 30, 2024)

Open Access

ABSTRACT

One sector that is experiencing changes in the current digital era is the financial sector, where payment transactions are starting to be carried out through digital systems, some of which use the QRIS system. Payment transactions via QRIS can speed up transactions and reduce operational costs, especially for commercial players. However, the use of QRIS has clearly given rise to what is called digital crime, which can harm users (QRIS consumers) by destroying the QR code and "undoing" the actions carried out by the perpetrator. This research uses qualitative research with data collection techniques through library research which is analyzed qualitatively. The results of the first research concluded that legal protection for QRIS users based on current regulations includes PJSP having valid legal status, PJSP must create a financial innovation ecosystem with good digital credentials in the financial services sector and be registered with the Financial Services Authority. OJK and QRIS users (consumers) enjoy rights based on the provisions of the Consumer Protection Law and the ITE Law. Second, the legal consequences of misusing consumer data in digital transactions using QRIS make the perpetrator liable for professional misconduct. For losses incurred, QRIS users can file a civil lawsuit or compensation through PJSP, as stipulated in Article 12, paragraph 1, Law no. 27, 2022 on personal data protection.

Keywords: Legal Aspects, Financial, Records, Digital, QRIS.

1. Introduction

When a group of young people born in 1980 began a revolution, the digital age began to develop. The emergence of digitalization marks the beginning of the digital information age, or the creation of new, more advanced technologies. Digitalization is a term used to describe the modernization or innovation of the use of technology. This is often associated with the existence of the internet and computer technology as tools that are able to do anything to facilitate human work (Pasca, n.d.).

The global phenomenon of the digital revolution has greatly changed the way of life and interaction of people, especially in the financial industry, in many countries, including Indonesia. The application of patterns of life and human interaction using various versions of the digital economy base is relatively easy and efficient. For people who are usually involved in relational model economic activities, this presents both opportunities and challenges, especially for those involved in various incarnations of the digital economy base, such as capital owners, platform service providers, and consumers *(Final Report Of Digital Financial Law Analysis And Evaluation, 2022).*

Technology is evolving so rapidly that it is changing human behavior and making transactions fully digital. Adopting digital technology isn't just a way to stay up-to-date with information; More importantly, digital technology can help people in various ways, including conducting financial transactions. Limited payments and financial system services, such as money transfers, storage of sums of money, and payment transactions, benefit service providers and customers when offered through the digital financial system. This reduces the danger of loss for customers and makes financial transactions fast, safe, and efficient (Pasca, n.d.). The banking world is one of the sectors that requires digital transformation. There are at least 3 (three) main aspects that encourage the development of digital banking transformation in Indonesia, namely digital opportunities, digital behavior, and digital transactions. The acceleration of digital banking in Indonesia is marked by the increasing use of digital payments through QRIS

* Fridayani
E-mail addresses: dosen02918@unpam.ac.id (Universitas Pamulang)

(Indonesian Standard for Quick Response Codes), (Saraswati, 2023).

From the perspective of digital transactions that are the focus of this study, Bank Indonesia (BI) notes that until October 2023, the nominal QRIS transaction will increase by 186.08% year-on-year (y-o-y) or reach IDR 24.97 trillion. Based on Bank Indonesia data, up to 83% of QRIS transaction volume is dominated by micro, small and medium enterprises (MSMEs). This number should have increased compared to previous years. Trade through QRIS can boost Indonesia's economic growth more effectively. Indeed, financial transactions through QRIS allow transactions to be faster and can reduce operational costs. According to Professor Dodi W. Irawanto, an expert on MSMEs and Human Resources Universitas Brawijaya (UB), said the digitalization system makes it easier for MSME players to increase their efficiency and productivity. With the presence of QRIS, MSME players no longer need to make conventional financial statements but can also be integrated with financial reporting platforms whose process is simpler. In addition, recording financial statements in real time can provide opportunities for efficiency with more accurate budget allocations (Fizriyani, n.d.).

Digital system financial transactions using QRIS clearly do not always have a positive impact on digital financial consumers, as mentioned above. Indeed, QRIS clearly has weaknesses that can be used by certain parties to obtain illegal benefits, thus potentially harming digital financial consumers. This condition is in line with voi.id quote that the use of QRIS for payment transactions will face the threat of digital crime. It is indeed very difficult for the human eye to distinguish real and fake QR codes. Indeed, it turns out that the seller's original official QR Code can be modified and added with virus and malware links that can steal consumer accounts (Redaksi, n.d.).

A new method of digital financial crime that uses the QRIS system through QR codes is called "quishing", which is a combination of QR codes and phishing, where perpetrators "lure" potential victims to obtain personal information. The way it works, when the victim scans the QR code, it will appear a simple text message, a list of apps, and even a map address. With this ability, potential victims will be directed by perpetrators to fake websites that are difficult to detect. The perpetrator then tricks the potential victim into downloading something into the device that actually harms the potential victim's device. Next, the attacker asks the potential victim to enter some login details, which the attacker then obtains. This type of "quishing" crime is on the rise because anyone with no special skills can easily create QR codes (Nano, 2024).

A real case in point is what happened to a mother named Rani, a roadside tortilla seller in the Bekasi area. Rani recently realizes that the income she earns from her sales is actually limited, which is only known a year later. From the search results, it is known that someone pasted a fake QRIS in their shopping cart. As a result of this incident, it is still unclear who the perpetrator of the fake QRIS installation is. The incident was reported to the local police by the victim but could not be dealt with due to difficulties in providing evidence. The victim then asked the bank where he kept the money to help find out the identity of the recipient of the money from a copy of his bank statement but to no avail. Because banks cannot provide confidential banking information to anyone.

Based on the problems arising from the use of QRIS as a digital payment transaction system above at least 2 (two) legal problems can be identified. First, consumers who are victims of QRIS fraud are in a weak position so that the government has an obligation to provide legal protection to QRIS users as consumers. Second, the QRIS system as a means of digital payment transactions causes digital crime by exploiting existing weaknesses in the form of fake QRIS and destroying it so that it can cause legal consequences.

2. Throritical Foundation and Hypothesis Development

Disruption Theory

Now, disruption is considered an opportunity, which means that not everyone can afford to resist disruptive new technologies in the world of e-commerce that will disrupt e-commerce platforms. It takes effort to find opportunities that can be exploited when e-commerce platforms are used as a means of marketing. Using this tool, neither party suffers any losses. According to Christensen, changing innovation always begins with observation, research, and after that, an idea emerges. You can make observations by looking at and paying attention to individuals involved in economic activities on e-commerce platforms. Upon investigation, it was revealed that the status of economic actors was not clearly defined because they generated temporary sales, making it difficult to find ways to ascertain whether any party suffered losses or not. So, it is important to have a concept as the first step of innovation to deal with these problems, such as providing legal guarantees to economic actors related to the failure of e-commerce platforms. Thus, everyone has the opportunity to sell it, even if only for a short period of time, as long as there is a guarantee of legal certainty. Community creativity and entrepreneurship will be stimulated by the ease of licensing for gig economy actors, so they can make online purchases and sales safely. In short, Doi A's great innovation in digital transformation is its ability to reduce the complexity and cost of difficult processes. In 2020, Ramli quoted Kasali (2017) who talked about the importance of producing quality and accessible innovations at affordable prices through good product development, systems, and management.

According to the concept of disruption, Bank Indonesia has introduced a QR code standard that can be used for payments using cryptocurrency or mobile banking applications. This QR code is known as the Indonesian Standard QR Code (QRIS) and is

regulated in Decree Regulation No. 21/18/Padg by Members of the Board of Governors of Bank Indonesia. In 2019, the National Payment Standard Quick Response Code was implemented which aims to increase efficiency and speed in payment processing across countries. QRIS has transformed the conventional payment system in the fintech industry by introducing barcodes as its replacement, creating a major breakthrough.

Consumer Law Protection Theory

Consumer protection can be described as "all efforts made to uphold legal justice in protecting consumer rights", as stipulated in Article 1 paragraphs 1 and 2 of Law Number 8 of 1999 concerning Consumer Protection. A person who utilizes products or services offered by a company for personal, family, other people, or other animal purposes is referred to as a consumer.

According to Abdul Halim Barkatullah reported by Vivek Sood, legal protection of consumers is becoming increasingly important along with the increasing level of global competition. Consumers are at a disadvantage in negotiations due to the abundance of products and services, and legal protection is needed in the face of competition. According to Hans W. Misklizt, there are basically two (2) consumer protection policy approaches that can be used. First, it complements the law, in particular the law that obliges companies to provide all available information to customers (right to information). Second, laws related to compensation, especially those that protect consumers' financial interests, relate to their right to health and safety (Panjaitan, 2021).

Digital Transactions.

Digital transactions are terms used to describe a type of virtual payment made through devices, gadgets, and applications or websites provided by service providers. According to Article 1 Number 2 of Law of the Republic of Indonesia Number 1 of 2024 which is the second amendment of Law Number 11 of 2008 concerning Electronic Information and Transactions, all actions carried out using computers and networks are considered valid. Therefore, digital transactions are the same as electronic transactions. Other documents that are on the computer are in digital form. There are several popular digital payment systems in Indonesia such as Flip, OVO, Go-pay, DANA, Sakuku, Link Aja, Shopee pay, and others (Nurohman et al., 2022).

QRIS

The Indonesian Quick Response Code (QRIS) standard is a combination of various types of QR from various payment system service providers (PJSP) that use QR codes. QRIS was developed by the payment system industry in collaboration with BI to make the transaction process easier, faster and safer using QR codes.

Picture 1. QRIS example

QR codes are technological advancements that facilitate the transmission of large amounts of data between devices quickly, efficiently, and easily, especially in financial transactions. Just by scanning the merchant's QR code and completing the payment transfer, customers can make cashless payment transfers using QR code payments (Sinaga et al., 2023). Soon (2008) claims that Denso Wave invented the QR code, which is a type of matrix code or two-dimensional barcode. This Japanese business introduced QR codes in 1994; Its main purpose is to make it easy to read by scanners.

QR code stands for "Quick Response" and is used to send information and receive quick responses. His reaction remained unchanged. Unlike barcodes that can only store data horizontally, QR codes can store data automatically and can hold more data than barcodes (Gufran et al., 2023). Jawi & Supriyono (2018) stated that a quick response code or QR code is a two-dimensional graphic that represents data in text form with the aim of conveying information quickly and receiving a fast response. The main feature of QR codes is that they are easy to read by scanners (FIDYA, 2023).

3. Research Methods

This research article consults with Mamahit & Urumsah (2018) using qualitative methods with a literary research approach, including observation and review of information related to the research topic. The author then combines the method with previous research related to this research to explain an upcoming event (Arianto & Octavia, 2021).

Primary and secondary legal papers serve as secondary data sources for data collection. The main legal documents in question are: Bank Indonesia Regulation Number 18/40/PBI/2016 concerning Payment for Transaction Processing; Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions; Indonesian Banking Regulation No. 20/6/PBI/2018 on Cryptocurrencies, Board of Governors Regulation Number 21/18/Padg/2019 concerning the Implementation of the National Payment Standard Quick Response Code; and other relevant regulations relating to this matter. Researching. Document research is used to develop secondary legal documents. Studying books, papers, research journals, online journals, and other literature sources related to the topic is

how literary research is carried out (Fauziyah & Rochayatun, 2023).

4. Results Of Research and Discussion

Legal Protection for QRIS Users

QRIS is a QR code format created to facilitate digital payment transactions using cryptocurrency applications, digital wallets, and mobile banking services in Indonesia. Board of Governors Regulation No. 21/18/PADG/2019 on the Implementation of the National Rapid Response is currently the legal basis stipulated by Bank Indonesia for the use of QRIS as a digital payment system in Indonesia. Standard code is the rules to be followed in writing code. in terms of payment (PADG number 21/18/2019). The use of QRIS as a digital payment method involves various parties, such as Payment System Service Providers (PJSP), switching institutions, merchant collectors, National Trade Archives (NMR), issuers, consumers, sellers, and QRIS users.

QRIS, as the implementation of financial technology in Indonesia, has a close relationship with PBI Number 19/12/2017 which regulates the implementation of financial technology. The PBI explains the goals to be achieved. Initially, in order to obtain varied needs from the community, including opening opportunities for access to financial services and transaction processes. Furthermore, reducing the likelihood of risks to the financial system through control measures. Third, support the sustainable development and merger of national economies by creating stability in the currency, stability in the financial system, and building trust in an efficient, barrier-free, secure, and reliable payment system. The next point is to ensure consumer protection when using financial technology.

When adopting QRIS as a payment method, consumers who use this service need to get special legal protection. Bank Indonesia Regulation dated 19th December 2017 states that financial technology providers using QRIS must implement consumer protection principles in using QRIS. The principles of consumer protection in the financial services sector have been explained in Article 2 of the Financial Services Authority Regulation Number: 1/POJK.07/2013 (POJK No. n On July 1, 2013, three main principles have been implemented, namely openness, fair handling, and trust. In order to maintain the confidentiality and security of consumer data and information, as well as handle complaints and solve consumer problems in an easy, fast, and effective way. Judging from the example of a fraud situation presented at the beginning of the article, it can be clearly seen that the need for legal protection for QRIS users is related to the security of consumer data and information as well as the handling of complaints in financial cases that harm consumers. The amount of money obtained from counterfeiting through QRIS, a form of digital crime, was obtained.

The security aspect of using QRIS for digital transactions must be met by QRIS operators as the main prerequisite for QRIS users in terms of security. Bank Indonesia is responsible for complying with the requirements stipulated in Bank Indonesia Regulation No.18/40. This paragraph talks about Bank Indonesia Regulation (PBI) Year 2016 concerning the implementation of payment transaction processing, which is indicated as PBI Number. To ensure the security of transactions made through QRIS, especially in terms of personal data protection of QRIS users managed by PJSP, important steps need to be taken. PBI Certificate 18/40/2016 notes that PJSP has the responsibility to maintain the security of information on QRIS usage. In addition, PJSP participation in providing and regulating payment facilities through QRIS has been regulated by Bank Indonesia with the aim of creating a secure and regulated payment system, in accordance with all applicable laws in Indonesia and obtaining legal permits. Justification against all forms of carelessness and rule-breaking behavior. Meanwhile, the customer's position in transactions using QRIS is in accordance with the responsibilities and roles of PJSP. Article 4 Number 1 of Law Number 8 of 1999 stipulates that consumers have the right to obtain correct information and ensure their security.

In an effort to strengthen public trust and improve QRIS performance in the digital payment system, the Financial Services Authority (OJK) has enacted laws regulating the security of QRIS use, in addition to actions taken by Bank Indonesia. In Article 37(1) of the Regulation of the Financial Services Authority of the Republic of Indonesia Number ..., it is explained that... In accordance with the Financial Services Authority Regulation Number 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector, payment service provider institutions (PJSP) are required to work together to develop a cooperation structure that allows the development of a digital financial innovation ecosystem to be implemented in payment systems used by financial institutions. To perform its digital financial support function, PJSP must first go through a registration process at OJK.

The importance of maintaining the security of QRIS user data is very large, therefore, the government needs to protect the data by issuing Law Number 27 of 2022 concerning Personal Data Security which in Article 54 paragraph (2) outlines the existence of officials and agents who aim to ensure the security of the data. Questions about QRIS transactions held by PSJP. In accordance with these regulations, PJSP must maintain the security of customer information related to the use of QRIS in the process of processing personal data. PJSP needs to be aware of the potential risks to customer information related to processing transactions using QRIS. PJSP also examines transactions, including what is involved in the transaction, the data used, the context of the transaction by QRIS users, and the purpose of processing the transaction.

Regarding the handling of complaints of QRIS users who suffer losses due to QRIS violations, PJSP is required to provide guidance through available information facilities regarding

complaints or complaint procedures that consumers can use to exercise their rights protected by law. This effort refers to the process of re-socializing the process of solving problems that arise in the payment system using QRIS. This is related to the case that occurred at the scene, where there are still many people who do not know how to use QRIS properly and are confused whether they are deceived by fake QRIS or not. Therefore, complaints regarding these problems can be submitted to PJSP as a payment service provider using QRIS (Telkom, 2022).

From the previous explanation, it can be concluded that PBI No.18/40/2016 regulates QRIS transaction security requirements. QRIS users who are also customers of digital transaction services will have legal certainty while utilizing QRIS to pay merchants thanks to these legal provisions. In addition to being regulated in PBI Number 18/40/2016, the security requirements for using QRIS as a payment system are also in accordance with UUPK Number 8 of 1999 which regulates consumer rights, one of which is the right to guarantees. — when consuming a product or service. Information system audit reports from independent auditors using security control procedures are evidence of PJSP readiness to carry out secure transaction process.

As the payment system regulator, Bank Indonesia is responsible for overseeing the implementation of payment system services and changes in organizational functions to legally protect QRIS customers. In order to stimulate economic growth and ensure structured policy, Bank Indonesia is supervising digital transactions through QRIS by providing an integrated payment system and policy framework to regulate the use of rupiah currency. To ensure resilience and provide legal protection for QRIS users, there are two types of supervision applied, namely direct supervision and indirect supervision. Routine inspections (field observations) conducted by Bank Indonesia are one of the elements of direct supervision. An example of indirect monitoring is when we request data, reports, documentation, and explanatory information about the QRIS transaction process. Monitoring is the main indicator to determine the success of the company's operations. In addition, Bank Indonesia's QRIS utilization also provides benefits in terms of supervision of consumer protection and clarity in legal matters.

Misuse of Consumer Data in Transactions Using QRIS.

The development of information technology in today's life is inevitable, because the development of information technology will follow the progress of science. Every new development that is raised aims to have a positive impact on human life. Not always the development of information technology has a positive impact on society, especially for economic entities that use digital systems in conducting financial transactions. In response, digital criminals are trying to adapt to this technological evolution to find loopholes in the digital payment system. Quishing is one form of digital crime that has become more prevalent in recent times. This crime was carried out through Quick Response Codes (QR Codes) with the aim of robbing QRIS users' personal data. It is important to maintain the confidentiality of personal data and the security of funds to avoid this threat. This text refers to data storage at QRIS user banks.

Misuse of personal data can be done by individuals or by PJSP itself because it is related to the personal data of consumers it manages. Therefore, based on Article 40 paragraph (2) of Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), PJSP is obliged to create favorable conditions for financial transactions through QRIS to protect QRIS users. Data is consumers who use QRIS in accordance with the law.

The emergence of digital crime cases with the term "quishing" mentioned in the introduction occurred due to the misuse of QRIS users' personal data. This is expressly prohibited by the ITE law which prohibits illegal access to other people's data through electronic systems to obtain infringing information. To express again the content of this text, we can convey it in the following way: The only text here is "n". security system referred to in Article 46 paragraph (2) of the ITE Law. In addition, there is a clear provision in the ITE Law which states that stealing QRIS user data is prohibited, unless it is done by the authorities through a valid legal process. Individuals who suffer losses as a result of breaking the law, have the right to file a claim for damages, while the offender must be held accountable for his actions. Any act of violating QRIS User's data privacy can be considered as an act of stealing identity. Identity theft refers to actions that involve illegally harvesting someone's personal data and using that information for personal gain or the benefit of others. The importance of personal data security is increasingly questioned because almost all QRIS user information is stored online, which makes data theft easier to do. Theft of individual personal information is one form of illegal action (Rumlus & Hartadi, 2020).

In addition to digital crime cases, an example in this case is the "quishing" model, which is QRIS forgery carried out by someone with the aim of diverting the transfer of funds received to the perpetrator's account. By forging QRIS, the author has violated the provisions of Article 31 of the ITE Law which regulates falsification of electronic information and/or electronic documents at the risk of criminal sanctions under the ITE Law, if proven to prove that the author committed falsification of its use. . by QRIS. QRIS. In addition, QRIS counterfeiting is subject to criminal sanctions for violating Article 49 of Law Number 10 of 1998 concerning the Banking Industry related to criminal acts in the payment system sector.

Incidents of misuse of consumers' personal data during digital transactions through QRIS and QRIS counterfeiting resulted in legal repercussions in response to the practice. The legal consequences that arise are legal duties that must be borne by those who misuse data. The responsibility applied is a consequence of mistakes made or in response to established principles, mainly based on the element of error. According to this principle, there is a need to give accountability to individuals or groups under supervision only if there is evidence of wrongdoing committed by them (Umboh, 2018). In the act of assuming this responsibility, data users are obliged to bear losses caused by their negligence. Evidence that the party using the data incorrectly must be presented by the loss-making victim. This task specifically focuses on parties who make mistakes by violating consumer data in QRIS transactions. According to Shidarta (2000), this principle posits that a person can only be held accountable if there is evidence of his guilt.

Legal consequences for individuals or small businesses that take advantage of consumer information in QRIS include compensation payments and legal processes in accordance with Article 12 paragraph (1) of Law Number 1 of January 27, 2017 concerning Protection of Personal Data Rights. The filing of a lawsuit made by someone who feels that they have suffered a loss cannot be declared valid. The first and third paragraphs of Article 67 of the Personal Data Protection Act (PDP) provide for additional legal consequences in addition to court proceedings and financial compensation. Additional criminal offences are terms used to describe the taking of money or property obtained through criminal activities and the payment of compensation.

In fact, anyone who feels aggrieved as a result of data misuse will be affected by the law. As a QRIS customer, everyone has the right to guarantee the legal security of their position and safeguard their data. The filing of a lawsuit against an illegal act is carried out through the District Court, and the aggrieved party can file a complaint to obtain compensation. Before submitting a complaint report to Bank Indonesia, the customer first submits it to PJSP.

5. Conclusion

1. Legal protection provided by the state to QRIS users based on applicable regulations, including PJSP having a valid legal status, PJSP must create a digital financial innovation ecosystem both in the financial services sector and registered with OJK, QRIS users. (consumers) are entitled to enjoy their rights under the provisions of the Consumer Protection Law and the ITE Law.
2. Malpractice perpetrators face legal repercussions if their consumer data is misused in digital transactions through QRIS. QRIS users can claim compensation through PJSP or file a civil lawsuit for losses suffered, in accordance with the provisions of Law Number 27 of 2022 concerning Personal Data Protection, especially Article 12 paragraph.

Research Limitation

This research was conducted with several research limitations encountered by researchers, which of course can affect the results of the study, including the following:

1. The research conducted by the author is qualitative research, only taking supporting data from a few typical cases of online media.
2. Researchers do not examine all legal aspects of digital financial transactions using QRIS but limit themselves to the protection and legal consequences of using QRIS users' personal data in the context of using QRIS without permission.

Implication

The implications of the results of the research that the author conducted are as follows 1. QRIS is a fake digital transaction medium and digital criminals use a "quishing" model through the actor's Quick Response Code that can harm QRIS users (consumers) by reducing their bank fund balances. 2. Consumers are careful in using QRIS and do not carelessly provide personal data to reduce fraudulent practices through the QRIS facility.

References

Arianto, N., & Octavia, B. D. A. (2021). Pengaruh Kualitas Pelayanan dan Distribusi terhadap Keputusan Pembelian. *Jurnal Disrupsi Bisnis*, *4*(2), 98–107.

Fauziyah, A. N., & Rochayatun, S. (2023). The Quality Of Internal Audit's Role, Good Corporate Governance, And High-Quality Corporate Value: A Literature Review. *Proceedings of the International Conference of Islamic Economics and Business (ICONIES)*, *9*(1), 243–252.

FIDYA, P. (2023). *Pengaruh Literasi Keuangan Digital, Kebermanfaatan, dan Daya Tarik Produk Terhadap Penggunaan E-Wallet (DANA) Education Pada Masyarakat Desa Natar*.

Fizriyani, W. (n.d.). *83 Persen Transaksi QRIS Didominasi Pelaku UMKM*. Retrieved January 10, 2024, from https://ekonomi.republika.co.id/berita/rykauh502/83-persen-transaksi-qris-didominasi-pelaku-umkm

Gufran, M. I., Natsir, M., & Tajuddin, T. (2023). Determinan Tingkat Penggunaan Quick Response Indonesian Standard Di Kota Kendari. *Value Added: Majalah Ekonomi Dan Bisnis*, *19*(2), 89–94.

Laporan Akhir Analisis Dan Evaluasi Hukum Keuangan Digital. (2022). https://bphn.go.id/data/documents/2022_keuangan_digital.pdf

Nano, V. (2024). *Modus Penipuan Pakai Kode QR di HP, Rekening Auto Ludes*. https://www.cnbcindonesia.com/tech/20240203192826-37-511477/modus-penipuan-pakai-kode-qr-di-hp-rekening-auto-ludes

Nurohman, Y. A., Qurniawati, R. S., & Ahzar, F. A. (2022). Pembayaran Digital Sebagai Solusi Transaksi Di Masa Pandemi Covid 19: Studi Masyrakat Muslim Solo Raya. *Among Makarti*, *15*(2).

Panjaitan, H. (2021). *Hukum Perlindungan Konsumen*. Jala Permata Aksara.

Pasca, K. T. T. (n.d.). *Masa Depan Uang Digital di Indonesia*.

Redaksi. (n.d.). *Kelebihan dan Kekurangan QRIS Beserta Cara Membuatnya, Pelaku UMKM Wajib Tahu!* Retrieved January 15, 2024, from https://voi.id/teknologi/265327/kelebihan-dan-kekurangan-qris

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *Jurnal Ham*, *11*(2), 285–299.

Saraswati, A. (2023). Peta Persaingan Bank Menuju Digital.

Sinaga, I. S. A., Yusrizal, Y., & Rahmadani, S. (2023). Analisis Manajemen Resiko Penggunaan Digital Payment:(Studi Kasus Pada PT. Bank Syariah Indonesia, Tbk KC Medan S. Parman). *JIKEM: Jurnal Ilmu Komputer, Ekonomi Dan Manajemen*, *3*(1), 647–685.

Telkom, I. (2022). *Service Centre QRIS Satu QR Code untuk Semua Payment*. https://qris.id/homepage/qris-service-center.