

## THE EFFECT OF SECURITY, RISK PERCEPTION, AND CONSUMER PROTECTION ON QRIS USER LOYALTY WITH THE MEDIATING ROLE OF TRUST

Farrel Azidan Najib<sup>1</sup>, Weni Novandari<sup>2</sup>, Isti Riana Dewi<sup>3</sup>, and Ana Nur Faizah<sup>4</sup>

<sup>1-3</sup>Management, Faculty of Economics and Business, Jenderal Soedirman University, Indonesia

<sup>4</sup>Bank Indonesia, Purwokerto Representative Office, Indonesia

\*Email corresponding author: [farrel.najib@mhs.unsoed.ac.id](mailto:farrel.najib@mhs.unsoed.ac.id)

**Article Information:** Received – June 25, 2026, Published --- August 10, 2026

---

### Abstract

Advances in digital technology are driving the transformation of payment systems from cash transactions to digital payments, one of which is through the Quick Response Code Indonesian Standard (QRIS). The use of QRIS in Indonesia, particularly in the Banyumas Regency, continues to see significant growth. However, there are still several issues regarding its use, including the potential for digital fraud, data breaches, and low levels of trust among some users toward digital payment systems. This study aims to analyze the influence of security, perceived risk, and consumer protection on QRIS user loyalty, with trust serving as a mediating variable. The study employs a quantitative approach using a survey method, distributing questionnaires to 80 QRIS users in the former Banyumas Residency region, which includes Banyumas, Cilacap, Purbalingga, and Banjarnegara Regencies. The sampling technique uses purposive sampling, with data analysis conducted using Structural Equation Modeling-Partial Least Squares (SEM-PLS). The results of the study indicate that security and consumer protection have a significant positive effect on the trust and loyalty of QRIS users, whereas perceived risk has a negative effect on user trust. Furthermore, trust was found to mediate the effects of security, perceived risk, and consumer protection on QRIS user loyalty. The research findings are expected to provide a more comprehensive understanding of the factors influencing QRIS user loyalty, as well as offer theoretical contributions to the development of digital payment system studies and practical insights for service providers and regulators in enhancing security and trust regarding the use of QRIS.

**Keywords:** QRIS, security, perceived risk, consumer protection, trust, user loyalty

---

### INTRODUCTION

The development of payment systems has undergone a significant transformation in line with the rapid advancement of digital technology (Fahimah & Harsono, 2023). Payment systems, which are one of the pillars supporting financial system stability, have shifted from cash-based transactions toward digital payment or electronic money (e-money) (Terantang et al., 2019). This shift has been driven not only by technological innovation but also by changes in societal behavior that increasingly prioritize convenience and speed in transactions (Alawan et al., 2016). Digital payment systems also allow people to transact without spatial or time constraints, thereby increasing the flexibility of economic activity (Bank Indonesia, 2020). Digitalization of the payment system has therefore become an important driver of technology-based economic growth.

In Indonesia, one important innovation in the digital payment system is the Quick Response Code Indonesian Standard (QRIS), developed by Bank Indonesia (Bank Indonesia, 2020). QRIS is a national QR code standard that integrates various digital payment methods into a single uniform system (Bank Indonesia, 2020). QRIS allows users to make payments through various digital wallet applications and mobile banking services, so that they no longer need to download or use a different payment application for every merchant (Auliandari et al., 2022). QRIS also makes it easier

for business actors, particularly micro, small, and medium enterprises, to accept digital payments more efficiently (Bank Indonesia, 2020).

**Table 1. QRIS Transaction Volume in the Former Banyumas Residency (February–April 2026)**

| Regency                  | February          | March             | April             |
|--------------------------|-------------------|-------------------|-------------------|
| Banjarnegara             | 999,175           | 1,888,916         | 2,614,329         |
| Banyumas                 | 6,724,008         | 8,862,316         | 11,191,881        |
| Cilacap                  | 6,012,871         | 3,755,120         | 3,828,626         |
| Purbalingga              | 1,826,944         | 2,237,275         | 1,913,636         |
| <b>Total QRIS Volume</b> | <b>15,562,999</b> | <b>16,743,627</b> | <b>19,548,472</b> |

*Source: (Bank Indonesia Purwokerto, 2026).*

According to Goodstats data for the fourth quarter of 2025, QRIS was the best-performing payment system in Indonesia, recording a transaction volume growth of 139.9% year-on-year with 59.53 million users and 42.75 million merchants (Shafidhya, 2026). This growth was also reflected in the former Banyumas Residency (Purwanto, 2026); the number of QRIS merchants in the Banyumas Raya area reached 626,687 units as of January 2026 (Purwanto, 2026). As shown in Table 1, QRIS transaction volume in the region increased by 3,985,474 transactions from February to April alone. Joyosemito (2025) further reports that QRIS transaction volume in Banyumas Raya has risen sharply over the past three years, from 10,005,942 transactions in 2023 to 35,314,191 transactions in 2024, and further to 90,715,971 transactions in 2025.

Despite this rapid adoption, security concerns and the possibility of fraud remain a major issue (Yudiana, 2023). As digital transactions increase, cybercriminals continue to modify their methods, including counterfeiting QR codes, creating malicious links, and redirecting payments to unauthorized accounts (Huzair, 2025). In recent years, cybercrime cases such as phishing, data theft, and QR code manipulation have become more frequent; the latest scheme uses counterfeit QR codes so that a victim's account is drained the moment the code is scanned (Dewi, 2026). If left unaddressed, such problems can erode public trust in digital payment systems (Saputra & Wahyuni, 2025).

In the academic literature, security is recognized as an important factor influencing user trust in digital systems (Damghanian et al., 2016). Security refers to a system's ability to protect user data and information from unauthorized threats (Chawla & Kumar, 2021). A high level of security increases users' sense of safety and thereby encourages trust in digital services (Damghanian et al., 2016); conversely, when a system is perceived as unsafe, users tend to reduce or even abandon its use (Rachma & Noorlailie, 2018).

Perceived risk is another factor that shapes consumer behavior in adopting digital payment technology (Damghanian et al., 2016). Perceived risk reflects the level of uncertainty users associate with a possible loss in a transaction (Rachma & Noorlailie, 2018), such as loss of funds, leakage of personal data, or system failure (Chawla & Kumar, 2021). Previous studies show that perceived risk has a negative effect on trust: the higher the perceived risk, the lower the level of user trust (Damghanian et al., 2016).

Consumer protection also plays an important role in building user trust (Saputra & Wahyuni, 2025). Consumer protection covers aspects such as data security, information transparency, and clear and effective dispute-resolution mechanisms (Saputra & Wahyuni, 2025); adequate protection makes consumers feel safer when transacting digitally (Chawla & Kumar, 2021), so that consumer protection functions not merely as regulation but also as a behavioral driver.

Trust is a key factor in determining the success of digital payment system adoption (Damghanian et al., 2016). In an uncertain digital transaction environment, trust becomes the foundation that enables interaction between users and service providers (Chawla & Kumar, 2021). Prior research shows that trust has a positive effect on consumer loyalty: consumers with a high level of trust tend to continue using the service (Saputra & Wahyuni, 2025).

Although various studies have examined the relationships among these variables, previous findings remain inconsistent (Perdani et al., 2025). Some studies find that perceived risk does not directly affect consumer behavior but instead operates through trust as a mediating variable (Perdani et al., 2025), while others find that perceived risk can directly affect continuance decisions (Putritama, 2019). Differences also remain regarding the role of trust across studies (Saputra & Wahyuni, 2025), indicating a research gap that warrants further investigation. In addition, most previous studies have focused on the e-commerce and mobile banking context (Chawla & Kumar, 2021), while research specifically addressing the QRIS payment system remains relatively limited (Bank Indonesia, 2020), even though QRIS has unique characteristics as an integrated, nationally standardized payment system.

Based on this background, this study offers novelty by integrating security, perceived risk, and consumer protection into a single research model to analyze their effect on user loyalty, with trust as a mediating variable, specifically within the QRIS context, which remains rarely examined in the literature. This article focuses exclusively on individual QRIS users (user consumers) in the former Banyumas Residency, distinguishing it from the broader thesis on which it is based, which also examined QRIS merchants (business consumers) as a separate respondent group. By narrowing the scope to individual users, this study is expected to provide a more focused theoretical and practical contribution to the development of digital payment system research.

## **LITERATURE REVIEW AND HYPOTHESIS FORMULATION**

### ***Literature Review***

The Stimulus–Organism–Response (S-O-R) theory developed by Mehrabian and Russell (1974) explains that individual behavior results from external stimuli that affect an individual's internal state (organism), which in turn produces a particular response. The theory is widely used in consumer-behavior research to explain how environmental factors shape psychological processes and behavior, and it provides a relevant framework for explaining user–technology interaction in digital payment systems such as QRIS (Eroglu et al., 2001). In this study, security, perceived risk, and consumer protection are positioned as the stimulus that users perceive when using QRIS; trust represents the organism, i.e., the internal psychological state formed after evaluating those stimuli; and loyalty represents the response, i.e., the behavioral outcome of that evaluation, reflected in users' intention to continue using QRIS, transact repeatedly, and recommend it to others.

Security is a condition free from potential danger or threat, whether intentional or unintentional (Marlien & Probo, 2010). In an information-systems context, security is the ability of a system to protect user data and information from threats that could damage the system or lead to data misuse (Hua, 2008). Kolsaker and Payne (2006) explain that security reflects users' perception of the reliability of a payment method and of the systems used to transmit and store data; when users feel that their personal and financial data are safe during a transaction, a sense of security is formed in every digital interaction (Flavian & Guinaliu, 2006). In the context of QRIS, security can therefore be understood as the level of user confidence that the system is able to protect information and transactions from unauthorized access and cybercrime. This study measures security using indicators adapted from Flavian and Guinaliu (2006) and Chawla and Kumar (2021), covering QRIS's ability to prevent unauthorized interception, protect transaction data from

hacking, maintain data integrity, provide information about its security features, and process transactions reliably.

Perceived risk is a user's subjective perception of the likelihood of loss or negative consequences when using a digital product or service (Featherman & Pavlou, 2003). It reflects the uncertainty consumers weigh when deciding whether to use a digital payment system (Rachma & Noorlailie, 2018) and may include the loss of funds, leakage of personal data, or system failure (Chawla & Kumar, 2021). Experimental evidence shows that perceived risk reduces users' tendency to adopt digital payment systems (Martin & Camarero, 2009). This study measures perceived risk using indicators adapted from Rachma and Noorlailie (2018) and Featherman and Pavlou (2003), covering the perceived risk of transacting via QRIS, the potential for financial loss, the possibility of unexpected problems, loss of control over payment-information privacy, and concern that unauthorized parties may misuse the user's account or funds.

Consumer protection refers to all efforts intended to guarantee legal certainty and protect consumers' rights in a transaction (Law No. 8 of 1999). In the context of digital financial services, consumer protection covers information transparency, transaction-security guarantees, and the availability of an effective complaint-resolution mechanism, and it helps create a sense of safety for users while also ensuring that service providers act honestly, fairly, and responsibly (Saputra & Wahyuni, 2025). This study measures consumer protection using indicators adapted from Rachma and Noorlailie (2018), Chow and Ho (2025), and Nasution and Suprayitno (2022), covering the clarity and completeness of transaction information, transparency about risks, availability of usage guidance, responsiveness to complaints, transaction-security guarantees, privacy protection, fairness of treatment, assurance that transactions are processed correctly, confidentiality of data, and ease of accessing QRIS-related services.

Trust is the degree of confidence that another party will act consistently and reliably in accordance with expectations (Gefen et al., 2003). Mcknight et al. (2002) define trust as the belief that allows a person to accept and use a technology after weighing its characteristics and inherent risks. In the context of digital payment systems such as QRIS, trust is particularly important because transactions involve an exchange of economic value that is vulnerable to various risks (Perdani et al., 2025). This study measures trust using indicators adapted from Rachma and Noorlailie (2018) and Perdani et al. (2025), covering confidence that QRIS can handle transactions properly, provides adequate information and access, is trustworthy overall as a payment instrument, is effective, and is secure.

Consumer loyalty is a strong commitment to continue using or repurchasing a product or service consistently in the future (Oliver, 1999), reflected not only in repeat-usage behavior but also in a positive attitude, emotional attachment, and trust toward the service. In the context of digital financial services, loyalty is important because it relates to service sustainability and long-term profitability, and customers who are loyal will continue using a service over the long term and build a sustained relationship with the provider (Saputra & Wahyuni, 2025). This study measures loyalty using indicators adapted from Rachma and Noorlailie (2018) and Perdani et al. (2025), covering the intention to continue using QRIS, increased frequency of use, willingness to recommend QRIS to others, commitment to continued use, and consistency of use across various transactions.

Prior studies on the relationships among security, perceived risk, consumer protection, trust, and loyalty in digital services show mixed results. Damghanian et al. (2016) found that perceived security positively affects trust while perceived risk negatively affects it in the context of online banking. Chawla and Kumar (2021) demonstrated that consumer protection strengthens trust and, in turn, loyalty in e-commerce. Saputra and Wahyuni (2025) confirmed that trust mediates the relationship between service quality, consumer protection, and loyalty. Meanwhile, Perdani et al. (2025) found that perceived risk influences continuance intention to use QRIS indirectly through trust among Generation Z, whereas Putritama (2019) found a direct effect of perceived risk on continuance decisions in mobile-payment fintech. This inconsistency, together

with the fact that most previous research has been conducted in the e-commerce and mobile-banking context rather than the QRIS context, forms the basis for the ten hypotheses developed in this study.

Loyalty reflects a user's commitment to continue using a service. Under the S-O-R framework, security acts as a stimulus that is cognitively processed into a sense of safety (organism) and produces continued usage as a response. Flavian and Guinaliu (2006) found that perceived security contributes to greater loyalty toward digital services, a result reinforced by Rachma and Noorlailie (2018) and Chawla and Kumar (2021), who showed that a high level of security increases both trust and loyalty.

***H1: Security has a positive effect on QRIS user loyalty.***

Perceived risk reflects users' assessment of potential loss when using a digital payment system. Under the S-O-R framework, perceived risk is positioned as a stimulus: the higher the perceived risk, the lower users' trust (organism), which in turn lowers their loyalty (response). Damghanian et al. (2016) found that perceived risk negatively affects usage behavior in digital services, a result corroborated by Azhara and Rozza (2024) and Chawla and Kumar (2021), who found that increased perceived risk lowers users' willingness to continue using a service, while Featherman and Pavlou (2003) identified perceived risk as a primary barrier to the continued adoption of technology-based services.

***H2: Perceived risk has a negative effect on QRIS user loyalty.***

Consumer protection creates a sense of safety and satisfaction among users of digital services. Under the S-O-R framework, consumer protection acts as a stimulus that signals assurance and certainty, which is processed into a sense of safety, trust, and satisfaction (organism), ultimately producing loyalty (response). Saputra and Wahyuni (2025) found that consumer protection significantly affects loyalty, particularly in digital-service contexts with a high degree of uncertainty, and Chawla and Kumar (2021) showed that adequate protection increases trust and subsequently loyalty.

***H3: Consumer protection has a positive effect on QRIS user loyalty.***

Trust is a central factor in the use of digital payment systems that involve risk and uncertainty, and system security is one of its key antecedents. Under the S-O-R framework, security is a stimulus that, through users' cognitive evaluation (organism), produces trust in the QRIS system. Flavian and Guinaliu (2006) found that perceived security significantly contributes to trust in online services, a finding supported by Chawla and Kumar (2021) and Damghanian et al. (2016), who identified security as a key determinant of trust in technology-based services.

***H4: Security has a positive effect on trust in QRIS.***

Perceived risk reflects the uncertainty users associate with potential loss when using a digital system, and higher risk tends to erode trust. Under the S-O-R framework, perceived risk as a stimulus is processed cognitively and, when high, diminishes the trust (organism) that would otherwise form. Featherman and Pavlou (2003) identified perceived risk as a primary barrier to trust formation in technology-based systems, and Chawla and Kumar (2021) found that increased perceived risk lowers users' trust in digital services.

***H5: Perceived risk has a negative effect on trust in QRIS.***

Consumer protection provides certainty and a sense of safety that supports the formation of trust. Under the S-O-R framework, consumer protection as a stimulus is processed into confidence that the system will act fairly and responsibly, which produces trust. Saputra and Wahyuni (2025) and Chawla and Kumar (2021) found that adequate consumer protection strengthens users' sense of safety and, subsequently, their trust in a digital service.

***H6: Consumer protection has a positive effect on trust in QRIS.***

Trust is the psychological mechanism that bridges users' evaluation of a system with their continued behavioral response. Under the S-O-R framework, trust as the organism directly shapes

loyalty as the response: once trust is established, users are more inclined to keep using the service, transact more frequently, and recommend it to others. Damghanian et al. (2016) and Saputra and Wahyuni (2025) confirmed that trust is a key determinant of loyalty toward digital services.

***H7: Trust has a positive effect on QRIS user loyalty.***

Beyond direct effects, this study also examines whether trust mediates the relationships between the three stimulus variables and loyalty. Gefen et al. (2003) indicated that trust mediates the relationship between technological antecedents, such as security, and repeat-usage behavior, suggesting that security does not create loyalty directly but rather through the trust it first builds.

***H8: Trust mediates the effect of security on QRIS user loyalty.***

Similarly, the effect of perceived risk on loyalty is expected to operate partly through trust: a high level of perceived risk lowers trust, which in turn lowers loyalty, consistent with the mediating role of trust described by Gefen et al. (2003) and the risk–trust relationship documented by Featherman and Pavlou (2003) and Chawla and Kumar (2021).

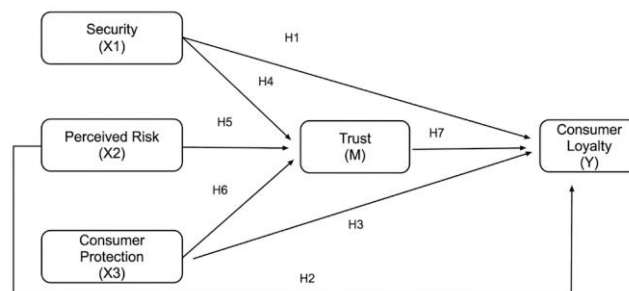
***H9: Trust mediates the effect of perceived risk on QRIS user loyalty.***

Finally, consumer protection is expected to affect loyalty not only directly but also indirectly by first strengthening trust. Chawla and Kumar (2021) found that adequate consumer protection strengthens users' sense of safety and trust, which subsequently drives loyalty, a mediating mechanism also suggested by Gefen et al. (2003).

***H10: Trust mediates the effect of consumer protection on QRIS user loyalty.***

## RESEARCH METHODS

Figure 1 presents the research model that summarizes the ten hypothesized relationships among security (X1), perceived risk (X2), consumer protection (X3), trust (M), and QRIS user loyalty (Y).



**Figure 1. Research Model**

This study uses a quantitative approach with a cross-sectional survey method (Sugiyono, 2022). The quantitative approach was chosen because it can objectively measure the relationships among variables through numerical data, allowing the ten research hypotheses — involving both direct effects and the mediating role of trust — to be tested empirically (Sugiyono, 2022). The cross-sectional survey method was used to collect data on the perceptions, attitudes, and behavior of QRIS users through a questionnaire distributed within a single period of time (Sujarweni, 2015).

The study was conducted in the former Banyumas Residency, comprising Banyumas, Cilacap, Purbalingga, and Banjarnegara Regencies. This location was selected because QRIS use in the area has grown rapidly, as described in the Introduction. The population of this study is all individual QRIS users (user consumers) in the former Banyumas Residency. Although the underlying thesis also surveyed QRIS merchants (business consumers) as a separate respondent group, this article reports and discusses only the individual-user model, in line with its narrower scope.

The minimum sample size was determined following the guideline proposed by Hair et al. (2021), which recommends a minimum sample of ten times the number of structural paths pointing to the most complex construct in the model. In this study, the loyalty construct receives the largest

number of structural paths (four), originating from security, perceived risk, consumer protection, and trust, so that the minimum required sample is  $10 \times 4 = 40$  respondents. To anticipate incomplete or unreturned questionnaires, 100 questionnaires were distributed to individual QRIS users. After a data-cleaning process to remove incomplete or inconsistent responses, 87 valid responses were obtained and used in the SEM-PLS analysis reported in this article.

The sampling technique used was purposive sampling (Suliyanto, 2018), applying the following criteria: (1) the respondent has used or is currently using QRIS as a digital payment method; and (2) the respondent resides in the former Banyumas Residency (Banyumas, Cilacap, Purbalingga, or Banjarnegara). Primary data were collected through two methods: online, using Google Forms, and offline, through physical questionnaires. The questionnaire was distributed via social media and messaging platforms (WhatsApp, X/Twitter, and Instagram) to reach respondents efficiently.

Data were collected using a closed questionnaire measured on a five-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree), to capture respondents' level of agreement with statements related to security, perceived risk, consumer protection, trust, and loyalty.

**Table 2. Operational Definition of Variables**

| Variable                 | Definition                                                                                                                      | Indicators (source)                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security (X1)            | Users' belief that the QRIS system can protect the confidentiality, integrity, and authenticity of their data and transactions. | Prevention of unauthorized data interception; technical capability to prevent hacking; protection of data integrity; availability of information on security features; reliability of transaction processing (Flavian & Guinaliu, 2006; Chawla & Kumar, 2021).                                                                                                                                         |
| Perceived Risk (X2)      | Users' subjective perception of the possibility of loss or negative consequences when using QRIS.                               | Perceived risk in transacting; potential financial loss; unexpected problems; loss of control over payment-information privacy; concern about unauthorized misuse of account or funds (Rachma & Noorlailie, 2018; Featherman & Pavlou, 2003).                                                                                                                                                          |
| Consumer Protection (X3) | The extent to which users feel protected — legally, informationally, and operationally — when using QRIS.                       | Clarity and completeness of transaction information; transparency of risk information; availability of usage guidance; complaint handling; transaction-security and reliability guarantees; privacy protection; fairness of treatment; assurance of correct processing; confidentiality of data; ease of access to services (Rachma & Noorlailie, 2018; Chow & Ho, 2025; Nasution & Suprayitno, 2022). |
| Trust (M)                | Users' confidence that QRIS is a reliable, secure payment system that meets their transaction needs.                            | Confidence in the system's ability to process transactions properly; adequacy of access and information; overall trustworthiness as a payment instrument; effectiveness; security (Rachma & Noorlailie, 2018; Perdani et al., 2025).                                                                                                                                                                   |

|                  |                                                                                             |                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Loyalty (Y) | Users' commitment to continuing to use QRIS consistently as a payment method in the future. | Intention to continue use; increased frequency of use; willingness to recommend to others; commitment to continued use; consistency of use across transactions (Rachma & Noorlailie, 2018; Perdani et al., 2025). |
|------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## RESULTS AND DISCUSSION

### *Respondent Profile.*

Of the 100 questionnaires distributed to individual QRIS users, 87 valid responses remained after data cleaning and were used in the analysis. Table 3 summarizes the demographic characteristics of these respondents.

**Table 3. Demographic Profile of QRIS User Respondents (n = 87)**

| Category       | Sub-category              | Percentage |
|----------------|---------------------------|------------|
| Gender         | Male                      | 40.23%     |
|                | Female                    | 59.77%     |
| Age            | ≤ 20 years                | 19.54%     |
|                | 21–30 years               | 74.71%     |
|                | 31–40 years               | 1.15%      |
|                | 41–50 years               | 4.60%      |
| Domicile       | Banyumas                  | 13.79%     |
|                | Banjarnegara              | 51.72%     |
|                | Cilacap                   | 12.64%     |
|                | Purbalingga               | 21.84%     |
| Education      | Senior high school        | 24.14%     |
|                | Diploma                   | 8.05%      |
|                | Bachelor's degree (S1)    | 67.82%     |
|                | Master's/Doctoral (S2/S3) | 0.00%      |
| Monthly Income | ≤ Rp1,000,000             | 40.23%     |
|                | Rp1,000,001–Rp3,000,000   | 32.18%     |
|                | Rp3,000,001–Rp5,000,000   | 17.24%     |
|                | Rp5,000,001–Rp10,000,000  | 3.45%      |
|                | Rp10,000,001–Rp15,000,000 | 3.45%      |
|                | > Rp15,000,000            | 3.45%      |

QRIS users in this study were dominated by female respondents (59.77%), compared with male respondents (40.23%), suggesting that QRIS has become part of everyday transaction habits widely used by women. In terms of age, most respondents were between 21 and 30 years old (74.71%), followed by those aged 20 years or younger (19.54%), 41–50 years (4.60%), and 31–40 years (1.15%). This pattern indicates that QRIS adoption is concentrated among younger, digitally adaptive users who are already familiar with smartphones, mobile banking, and digital wallets. By

domicile, most respondents resided in Banjarnegara Regency (51.72%), followed by Purbalingga (21.84%), Banyumas (13.79%), and Cilacap (12.64%). Most respondents held a bachelor's degree (67.82%), and 40.23% reported a monthly income of Rp1,000,000 or less, consistent with the relatively young, student-dominated age profile of the sample.

**Table 4. QRIS Usage Profile of Respondents (n = 87)**

| Question                                 | Category  | Percentage |
|------------------------------------------|-----------|------------|
| Duration of QRIS use                     | ≤ 1 year  | 9.20%      |
|                                          | 1–3 years | 44.83%     |
|                                          | ≥ 3 years | 45.98%     |
| Frequency of use per day                 | 1–3 times | 68%        |
|                                          | 5 times   | 16%        |
|                                          | > 5 times | 16%        |
| Still uses other digital payment methods | Yes       | 98%        |
|                                          | No        | 2%         |

Table 4 shows that respondents generally have substantial experience using QRIS: 45.98% had used QRIS for three years or more and 44.83% for one to three years, so that 90.81% had used it for over a year. In terms of intensity, 68% of respondents used QRIS one to three times a day, while 16% used it five times and another 16% used it more than five times per day. Furthermore, 98% of respondents still used other digital payment methods besides QRIS. These results indicate that respondents were experienced, active users who were familiar with the broader digital-payment ecosystem and were therefore well positioned to give an informed evaluation of the security, perceived risk, consumer protection, trust, and loyalty variables examined in this study.

#### **Measurement Model (Outer Model) Evaluation.**

Convergent validity was assessed through outer loadings and the Average Variance Extracted (AVE). All 30 indicators across the five constructs produced outer loadings between 0.730 and 0.870, exceeding the recommended threshold of 0.70, indicating that every indicator validly measures its intended latent construct. Table 5 presents the reliability and AVE results.

**Table 5. Convergent Validity and Reliability**

|                          | Cronbach's alpha | Composite reliability (rho_a) | Composite reliability (rho_c) | Average variance extracted (AVE) | Result |
|--------------------------|------------------|-------------------------------|-------------------------------|----------------------------------|--------|
| Trust (M)                | 0.873            | 0.874                         | 0.908                         | 0.663                            | Valid  |
| Security (X1)            | 0.872            | 0.878                         | 0.907                         | 0.662                            | Valid  |
| Loyalty (Y)              | 0.878            | 0.881                         | 0.911                         | 0.673                            | Valid  |
| Consumer Protection (X3) | 0.937            | 0.939                         | 0.946                         | 0.639                            | Valid  |
| Perceived Risk (X2)      | 0.880            | 0.882                         | 0.912                         | 0.675                            | Valid  |

As shown in Table 5, all five constructs recorded an AVE above the 0.50 threshold, ranging from 0.639 (consumer protection) to 0.675 (perceived risk), confirming adequate convergent validity. Reliability was also well established: Cronbach's alpha ranged from 0.872 to 0.937 and composite reliability (rho\_c) ranged from 0.907 to 0.946, both well above the 0.70 threshold, indicating that the indicators for each construct produced consistent responses.

Discriminant validity was examined using the Heterotrait-Monotrait Ratio (HTMT) and the Fornell-Larcker criterion. As shown in Table 6, all HTMT values for the user model were below the 0.90 threshold, with the highest ratio (0.843) found between trust and loyalty and the lowest (0.098) between security and consumer protection, indicating that all five constructs are empirically distinct.

**Table 6. Heterotrait-Monotrait Ratio (HTMT)**

|                                 | M     | X1    | Y     | X3    | X2 |
|---------------------------------|-------|-------|-------|-------|----|
| <b>Trust (M)</b>                |       |       |       |       |    |
| <b>Security (X1)</b>            | 0.655 |       |       |       |    |
| <b>Loyalty (Y)</b>              | 0.843 | 0.578 |       |       |    |
| <b>Consumer Protection (X3)</b> | 0.344 | 0.098 | 0.370 |       |    |
| <b>Perceived Risk (X2)</b>      | 0.528 | 0.135 | 0.525 | 0.166 |    |

Table 7 presents the Fornell-Larcker criterion, which compares the square root of each construct's AVE (diagonal, in bold) with its correlations with other constructs. Every construct's diagonal value exceeds its correlations with other constructs — for example, trust (0.815) exceeds its correlation with loyalty (0.723), security (0.575), consumer protection (0.316), and perceived risk (–0.468) — confirming that the measurement model satisfies the Fornell-Larcker discriminant-validity criterion.

**Table 7. Fornell-Larcker Criterion**

|                                 | M            | X1           | Y            | X3           | X2 |
|---------------------------------|--------------|--------------|--------------|--------------|----|
| <b>Trust (M)</b>                | <b>0.815</b> |              |              |              |    |
| <b>Security (X1)</b>            | 0.575        | <b>0.808</b> |              |              |    |
| <b>Loyalty (Y)</b>              | 0.723        | 0.493        | <b>0.772</b> |              |    |
| <b>Consumer Protection (X3)</b> | 0.316        | –0.035       | 0.327        | <b>0.774</b> |    |

---

|                            |        |        |        |       |              |
|----------------------------|--------|--------|--------|-------|--------------|
| <b>Perceived Risk (X2)</b> | -0.468 | -0.015 | -0.453 | 0.073 | <b>0.800</b> |
|----------------------------|--------|--------|--------|-------|--------------|

---

**Structural Model (Inner Model) Evaluation.**

A collinearity check on the inner model showed that all indicator VIF values ranged from 1.532 to 2.601, well below the 5.0 threshold, indicating that the user model is free from multicollinearity problems.

**Table 8. Coefficient of Determination ( $R^2$ )**

| Construct   | R-square | R-square adjusted | Category |
|-------------|----------|-------------------|----------|
| Trust (M)   | 0.679    | 0.668             | Moderate |
| Loyalty (Y) | 0.613    | 0.594             | Moderate |

Table 8 shows that security, perceived risk, and consumer protection jointly explain 67.9% of the variance in trust ( $R^2 = 0.679$ ), while security, perceived risk, consumer protection, and trust jointly explain 61.3% of the variance in loyalty ( $R^2 = 0.613$ ). Both values fall in the moderate category, which is considered adequate for consumer-behavior research given the many external factors that can influence user behavior.

**Table 9. Effect Size ( $f^2$ )**

|                          | M     | X1 | Y     | X3 | X2 |
|--------------------------|-------|----|-------|----|----|
| Trust (M)                |       |    | 0.223 |    |    |
| Security (X1)            | 0.477 |    | 0.093 |    |    |
| Loyalty (y)              |       |    |       |    |    |
| Consumer Protection (X3) | 0.682 |    | 0.187 |    |    |
| Perceived Risk (X2)      | 0.336 |    | 0.104 |    |    |

As shown in Table 9, consumer protection ( $f^2 = 0.682$ ) and security ( $f^2 = 0.477$ ) are the strongest contributors to trust, followed by perceived risk ( $f^2 = 0.336$ ). For loyalty, consumer protection ( $f^2 = 0.187$ ) and trust ( $f^2 = 0.223$ ) contribute the most, followed by perceived risk ( $f^2 = 0.104$ ) and security ( $f^2 = 0.093$ ).

**Hypothesis Testing.**

Hypothesis testing was conducted through a bootstrapping procedure with 5,000 resamples in SmartPLS 4. A hypothesis is accepted when the t-statistic exceeds 1.96 and the p-value is below 0.05. Table 10 presents the results for the seven direct-effect hypotheses (H1–H7).

**Table 10. Direct Effects**

|                                                 | Original<br>sample (O) | Sample<br>mean (M) | Standard<br>deviation<br>(STDEV) | T statistics<br>( O/STDEV<br> ) | P values |
|-------------------------------------------------|------------------------|--------------------|----------------------------------|---------------------------------|----------|
| Security (X1)<br>→ Trust (M)                    | 0.581                  | 0.570              | 0.060                            | 9.732                           | 0.000    |
| Security (X1)<br>→ Loyalty<br>(Y)               | 0.328                  | 0.329              | 0.108                            | 3.028                           | 0.002    |
| Perceived<br>Risk (X2) →<br>Loyalty (Y)         | -0.486                 | -0.481             | 0.063                            | 7.743                           | 0.000    |
| Perceived<br>Risk (X2) →<br>Loyalty (Y)         | -0.329                 | -0.336             | 0.091                            | 3.632                           | 0.000    |
| Consumer<br>Protection<br>(X3) → Trust<br>(M)   | 0.372                  | 0.375              | 0.073                            | 5.060                           | 0.000    |
| Consumer<br>Protection<br>(X3) →<br>Loyalty (Y) | 0.269                  | 0.276              | 0.081                            | 3.305                           | 0.001    |
| Trust (M) →<br>Loyalty (Y)                      | 0.296                  | 0.284              | 0.135                            | 2.199                           | 0.028    |

All seven direct-effect hypotheses were supported. Security had a significant positive effect on both loyalty ( $\beta = 0.328$ ;  $t = 3.028$ ;  $p = 0.002$ ; H1 accepted) and trust ( $\beta = 0.581$ ;  $t = 9.732$ ;  $p = 0.000$ ; H4 accepted), confirming that a stronger perception of QRIS security — including protection from data interception, resistance to hacking, and reliable transaction processing — raises both users' confidence in the system and their intention to keep using it. This result is consistent with Flavian and Guinaliu (2006), Rachma and Noorlailie (2018), and Chawla and Kumar (2021).

Perceived risk had a significant negative effect on loyalty ( $\beta = -0.329$ ;  $t = 3.632$ ;  $p = 0.000$ ; H2 accepted) and on trust ( $\beta = -0.486$ ;  $t = 7.743$ ;  $p = 0.000$ ; H5 accepted). This indicates that the more users perceive risks such as potential financial loss, unexpected problems, or loss of control over their information, the lower their trust in and loyalty toward QRIS, consistent with Damghanian et al. (2016), Featherman and Pavlou (2003), and Chawla and Kumar (2021).

Consumer protection had a significant positive effect on loyalty ( $\beta = 0.269$ ;  $t = 3.305$ ;  $p = 0.001$ ; H3 accepted) and on trust ( $\beta = 0.372$ ;  $t = 5.060$ ;  $p = 0.000$ ; H6 accepted), confirming that transparent transaction information, responsive complaint handling, and clear security and privacy guarantees strengthen both users' trust and their continued loyalty toward QRIS, in line with Saputra and Wahyuni (2025) and Chawla and Kumar (2021).

Finally, trust had a significant positive effect on loyalty ( $\beta = 0.296$ ;  $t = 2.199$ ;  $p = 0.028$ ; H7 accepted), showing that once users trust QRIS as a reliable and secure system, they are more likely to keep using it, use it more often, and recommend it to others — consistent with Damghanian et al. (2016) and Saputra and Wahyuni (2025).

Table 11 presents the results of the mediation (specific indirect effect) tests for H8–H10.

**Table 11. Mediation (Specific Indirect) Effects**

|                                             | Original<br>sample<br>(O) | Sample<br>mean<br>(M) | Standard<br>deviation<br>(STDEV) | T statistics<br>( O/STDEV ) | P<br>values |
|---------------------------------------------|---------------------------|-----------------------|----------------------------------|-----------------------------|-------------|
| Security →<br>Trust → Loyalty               | 0.172                     | 0.163                 | 0.080                            | 2.151                       | 0.032       |
| Perceived Risk<br>→ Trust →<br>Loyalty      | -0.144                    | -0.138                | 0.071                            | 2.041                       | 0.041       |
| Consumer<br>Protection →<br>Trust → Loyalty | 0.110                     | 0.106                 | 0.054                            | 2.042                       | 0.041       |

All three mediation hypotheses were supported. Security had a significant positive indirect effect on loyalty through trust ( $\beta = 0.172$ ;  $t = 2.151$ ;  $p = 0.032$ ; H8 accepted); because the direct effect of security on loyalty (H1) was also significant, trust functions as a partial mediator, meaning security affects loyalty both directly and indirectly through the trust it builds. Perceived risk had a significant negative indirect effect on loyalty through trust ( $\beta = -0.144$ ;  $t = 2.041$ ;  $p = 0.041$ ; H9 accepted); since its direct effect on loyalty (H2) was also significant, trust again acts as a partial mediator, showing that higher perceived risk lowers loyalty both directly and by first eroding trust. Consumer protection had a significant positive indirect effect on loyalty through trust ( $\beta = 0.110$ ;  $t = 2.042$ ;  $p = 0.041$ ; H10 accepted); given the significant direct effect found under H3, trust likewise partially mediates this relationship, indicating that consumer protection strengthens loyalty both directly and through the trust it fosters.

Overall, these findings confirm the Stimulus-Organism-Response framework in the QRIS context: security, perceived risk, and consumer protection function as external stimuli that shape trust as an internal psychological state, which subsequently drives loyalty as a behavioral response. The findings also show that, among individual QRIS users in the former Banyumas Residency, none of the hypothesized relationships reversed direction — security and consumer protection consistently strengthened trust and loyalty, while perceived risk consistently weakened both, underscoring that, for individual consumers, minimizing perceived risk while reinforcing security and protection mechanisms is central to sustaining QRIS loyalty.

## CONCLUSION

This study examined the effect of security, perceived risk, and consumer protection on QRIS user loyalty, with trust as a mediating variable, among 87 individual QRIS users (user consumers) in the former Banyumas Residency. Using SEM-PLS, all ten hypotheses were supported. Security and consumer protection have a significant positive effect on both trust and loyalty, while perceived risk has a significant negative effect on both. Trust itself has a significant positive effect on loyalty and partially mediates the effects of security, perceived risk, and consumer protection on loyalty, meaning that these three stimulus variables shape loyalty both directly and indirectly through the trust they build.

Theoretically, this study reinforces the relevance of the Stimulus-Organism-Response (S-O-R) framework for explaining behavior in the context of a nationally standardized digital payment system such as QRIS, and it provides empirical evidence that trust functions as a partial mediator between external stimuli and consumer loyalty. The findings also underline the importance of treating consumer protection as a distinct construct alongside security and perceived risk in models of digital-payment consumer behavior, an aspect that has received comparatively less attention in prior QRIS-related research.

Practically, the findings suggest several recommendations. For Bank Indonesia and payment-system regulators, continued strengthening of cybersecurity regulation — including transaction-encryption standards, multi-factor authentication requirements, and early-detection mechanisms for counterfeit QR codes — together with wider socialization of consumer-protection mechanisms such as dispute reporting and compensation guarantees, is warranted given that security ( $\beta = 0.581$ ) is the strongest driver of user trust. For payment-service providers and QRIS aggregators, proactively communicating the system's security features and improving the responsiveness of complaint-handling services are important, since the availability of security information and effective complaint resolution are both significant indicators in this study. For QRIS users, given that perceived risk significantly and negatively affects both trust and loyalty, improving digital financial literacy and understanding of QRIS's actual security features can help correct exaggerated risk perceptions and thereby support sustained, confident use of the system.

This study has several limitations. First, it uses a cross-sectional design, capturing user perceptions at a single point in time and therefore unable to capture how trust and loyalty evolve as the digital-payment ecosystem continues to develop. Second, the data rely on a self-reported Likert-scale questionnaire, which is susceptible to subjective response bias. Third, the analysis is confined to individual QRIS users in one regional context, the former Banyumas Residency, which may limit the generalizability of the findings to other regions or user segments.

Future research is encouraged to adopt a longitudinal design to capture changes in trust and loyalty over time, to apply mixed-methods approaches that combine quantitative testing with in-depth interviews for a richer understanding of user behavior, and to replicate or extend this model to other digital-payment platforms, such as mobile banking, e-wallets, or buy-now-pay-later services, as well as to broader geographic contexts, in order to assess the generalizability of the security–risk–protection–trust–loyalty relationships identified in this study.

## BIBLIOGRAPHY

- Alawan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2016). Consumer adoption of mobile banking in Jordan: Examining the role of usefulness, ease of use, perceived risk and self-efficacy. *Journal of Enterprise Information Management*, 29(1), 118–139. <https://doi.org/10.1108/JEIM-04-2015-0035>
- Auliandari, T., Azmi, Z., & Suriyanti, L. H. (2022). Determinan adopsi e-commerce dan pengaruhnya terhadap kinerja UMKM (studi kasus pada UMKM fashion di Pekanbaru). *Jurnal Akuntansi & Ekonomika*, 6(2). <https://doi.org/10.35915/accountia.v6i2.703>
- Azhara, R., & Rozza, S. (2024). Pengaruh persepsi risiko, persepsi keamanan, dan user experience terhadap loyalitas nasabah menggunakan aplikasi BSI Mobile. *Seminar Nasional Akuntansi Dan Manajemen*, 3.
- Bank Indonesia. (2020). Quick Response Code Indonesian Standard (QRIS). Bank Indonesia. <https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/ritel/kanal-layanan/qr/default.aspx>
- Chawla, N., & Kumar, B. (2021). E-commerce and consumer protection in India: The emerging trend. *Journal of Business Ethics*, 175, 649–663. <https://doi.org/10.1007/s10551-021-04884-3>
- Chow, M. Y. C. C., & Ho, S. P. S. (2025). Effects of financial consumer protection on brand love and brand advocacy. *Journal of Financial Services Marketing*, 30(2), 1–15. <https://doi.org/10.1057/s41264-025-00306-x>

- Damghanian, H., Zarei, A., & Kojuri, S. (2016). Impact of perceived security on trust, perceived risk, and acceptance of online banking in Iran. *Journal of Internet Commerce*, 15(3), 214–238. <https://doi.org/10.1080/15332861.2016.1191052>
- Dewi, I. R. (2026, January). Awas rekening ludes! Maling colong uang lewat QRIS. CNBC Indonesia.
- Eroglu, S. A., Machleit, K. A., & Davis, L. M. (2001). Atmospheric qualities of online retailing: A conceptual model and implications. *Journal of Business Research*, 54(2), 177–184.
- Fahimah, H. M., & Harsono, M. (2023). Literature review of the evolution of payment system paradigms: From cash to cashless with digital payment. *Sebelas Maret Business Review*, 7, 11–18. <https://doi.org/10.20961/shes.v6i3.81553>
- Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451–474. [https://doi.org/10.1016/S1071-5819\(03\)00111-3](https://doi.org/10.1016/S1071-5819(03)00111-3)
- Flavian, C., & Guinaliu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems*, 106(5), 601–620. <https://doi.org/10.1108/02635570610666403>
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50.
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51–90.
- Hair Jr., J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Partial least squares structural equation modeling (PLS-SEM) using R. Springer. <https://doi.org/10.1007/978-3-030-80519-7>
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Hua, G. (2008). An experimental investigation of online banking adoption in China. *Journal of Internet Banking and Commerce*.
- Huzair, I. (2025, December 11). Ancaman penipuan via QRIS: Tips aman menggunakan pembayaran digital. *Rakyat Sulsel*. <https://rakyatsulsel.fajar.co.id/2025/12/11/ancaman-penipuan-via-qris-tips-aman-menggunakan-pembayaran-digital/>
- InteractiveQRIS. (2025). Jangan sampai tertipu! Ini beda QRIS untuk bayar dan QR untuk transfer. <https://qris.interactive.co.id/homepage/blog-detail.php?lang=id&page=MTc1>
- Joyosemito, E. (2025). Tren penggunaan QRIS meningkat tajam di Banyumas Raya, ini buktinya. *iNews Purwokerto*. <https://purwokerto.inews.id/read/661130/>
- Kolsaker, A., & Payne, C. (2006). Engendering trust in e-commerce: A study of gender-based concerns. *Marketing Intelligence & Planning*, 20(4). <https://doi.org/10.1108/02634500210431595>

- Marlien, R., & Probo, Y. (2010). Pengaruh reputasi, privasi, dan keamanan terhadap kepercayaan (trust) pengguna internet di Semarang dalam sistem e-commerce. *Benefit: Jurnal Manajemen Dan Bisnis*, 14(2), 86–101.
- Martin, D., & Camarero, C. (2009). How perceived risk affects online buying. *Journal of Business Research*, 62(9), 901–908.
- Mcknight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359.
- Mehrabian, A., & Russell, J. A. (1974). *An approach to environmental psychology*. The MIT Press.
- Nasution, A. M., & Suprayitno, E. (2022). Pengaruh penggunaan e-banking dan perlindungan nasabah terhadap kepercayaan nasabah dengan literasi keuangan sebagai variabel moderasi. *Jurnal Ilmiah Ekonomi Islam*, 8(2), 1205–1213.
- Oliver, R. L. (1999). Whence consumer loyalty? *Journal of Marketing*, 63(4\_suppl1), 33–44.
- Perdani, T. A. M., Fitriati, A., Kusbandiyah, A., & Azizah, S. N. (2025). Pengaruh persepsi manfaat dan persepsi risiko terhadap niat penggunaan berkelanjutan QRIS yang dimediasi oleh kepercayaan pada Generasi Z. *Jurnal Akuntansi Fakultas Ekonomi (JAFM)*, 6(2), 791–808. <https://doi.org/10.38035/jafm.v6i2.1984>
- Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, 40(3), 879–891. <https://doi.org/10.3758/BRM.40.3.879>
- Purwanto, P. (2026, January). Merchant QRIS di Banyumas Raya tembus 626 ribu, UMKM makin go digital. *Suara Merdeka*. <https://www.suaramerdeka.com/ekonomi/0416831777/>
- Putritama, A. (2019). The mobile payment fintech continuance usage intention in Indonesia. *Jurnal Economia*, 15(2), 243–258. <https://doi.org/10.21831/economia.v15i2.26403>
- Rachma, A. M., & Noorlailie, S. (2018). Participation customer on e-commerce: Relationship perceived risk, security, trust, and consumer protection. *Journal of Economics, Business, and Accountancy Ventura*, 21(1), 121–132.
- Saputra, G. E., & Wahyuni, S. (2025). Service quality and consumer protection effect on loyalty: Trust as intervening variable. *International Journal of Business, Law, and Education*, 15(1), 17–24.
- Shafidhya, T. A. (2026). QRIS tumbuh pesat sepanjang 2025, jumlah pengguna tembus 59 juta orang. *Goodstats*. <https://goodstats.id/article/qris-tumbuh-pesat-sepanjang-2025-digunakan-lebih-dari-59-juta-orang-L9I0G>
- Sugiyono. (2022). *Metode penelitian kuantitatif, kualitatif, dan R&D* (2nd ed.). Alfabeta.
- Sujarweni, V. W. (2015). *Metodologi penelitian bisnis & ekonomi*. Pustaka Baru Press.
- Suliyanto. (2018). *Metode penelitian bisnis untuk skripsi, tesis, & disertasi*. Andi Offset.

Terantang, J., Awwaliyah, A., Astuti, M., & Munawaroh, M. (2019). Perkembangan sistem pembayaran digital pada era revolusi industri 4.0 di Indonesia. *Jurnal Manajemen Dan Bisnis Indonesia*, 4, 60–75.

Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.  
<https://peraturan.bpk.go.id/Details/45288/uu-no-8-tahun-1999>

Yudiana, A. A. (2023). Pengaruh penggunaan QRIS, pendapatan, tabungan dan gaya hidup terhadap perilaku konsumtif. *Jurnal Ilmiah Ekonomi*, 2(4), 739–746.