JURNAL EKONOMI DAN BISNIS
Journal homepage: www.ejournal.uksw.edu/jeb
ISSN 1979-6471 E-ISSN 2528-0147

Understanding the attributes of digital wallet customers: Segmentation based on perceived risk during the Covid-19 pandemic

Yudi Sutarso[a]*, Larasati Ayu Sekarsari[b], Ersa Annisatul Hidayati[c], Hane Andariksa[d], Meytita Zafira Putri[e]

[a] *Faculty of Economics and Business,Universitas Hayam Wuruk Perbanas, Surabaya, Indonesia; yudi@perbanas.ac.id**
[b] *Faculty of Economics and Business,Universitas Hayam Wuruk Perbanas, Surabaya, Indonesia; larasati.ayu@perbanas.ac.id*
[c] *Faculty of Economics and Business,Universitas Hayam Wuruk Perbanas, Surabaya, Indonesia; 2017710354@students.perbanas.ac.id*
[d] *Faculty of Economics and Business,Universitas Hayam Wuruk Perbanas, Surabaya, Indonesia; 2017710709@students.perbanas.ac.id*
[e] *Faculty of Economics and Business,Universitas Hayam Wuruk Perbanas, Surabaya, Indonesia; 2017710332@students.perbanas.ac.id*

ARTICLE INFO

Article History:
Received 12-05-2021
Revised 05-26-2022
Accepted 08-05-2022

Kata Kunci:
Risiko operasional, risiko sosial, risiko finansial, risiko keamanan, segmentasi, dompet digital, covid-19

Keywords:
Operational risk, social risk, financial risk, security risk, segmentation, digital wallet, covid-19

ABSTRAK

Penelitian ini menekankan pada pentingnya segmentasi pelanggan dompet digital, khususnya segmentasi yang didasarkan pada persepsi risiko pelanggan pada saat pandemi Covid-19. Kontribusi mendasar yang diharapkan dari studi ini adalah penjelasan konsep risiko dalam konteks dompet digital. Studi ini juga akan mengkonfirmasi faktor risiko dalam dompet digital dan pemetaan pengguna berdasarkan faktor persepsi resiko tersebut. Studi ini melibatkan 270 pengguna dompet digital sebagai sampel penelitian, yang di ambil menggunakan teknik purposive sampling. Keseluruhan sampel diambil di Surabaya yang dilakukan saat pandemi Covid-19 masih berlangsung. Dompet digital yang digunakan adalah layanan aplikasi OVO, Gopay dan Dana. Analisis dilakukan menggunakan analisis faktor, kluster dan uji beda. Temuan penting studi ini adalah faktor risiko pada dompet digital teridentifikasi terdiri dari faktor risiko keamanan, finansial, sosial dan operasional. Terbentuk tiga segmen pengguna berdasarkan risiko, yaitu klaster risiko rendah, sedang, dan tinggi. Masing-masing segmen memiliki karakteristik dan implikasi manajeral yang berbeda.

ABSTRACT

This research emphasizes the importance of digital wallet customer segmentation, mainly based on customer risk perceptions during the Covid-19 pandemic. The fundamental contribution of the study was to explain the concept of perceived risk in a digital wallet, also to confirm risk factors in digital

*Corresponding Author

wallets, and identify segments based on perceived risk factors. The respondents are 270 digital wallet users of OVO, Gopay, and Dana obtained in Surabaya, Indonesia, during the Covid-19 pandemic, which was taken using the purposive sampling technique. The multiple analysis data were carried out using factor analysis, cluster analysis, and difference test techniques. An essential finding of this study shows that perceived risk factors consist of security, financial, social, and operational risks. There are three segments based on the perceived risk: low-risk, medium-risk, and high-risk. Each segment has different characteristics and managerial implications.

INTRODUCTION

Digital wallet is one of the applications that have greatly benefited users in their online transactions, especially during the Covid-19 pandemic. Digital wallets are designed to offer customers speed, ease of use, efficiency, effectiveness, transparency, and accessibility (Kaur et al., 2020). Users benefit because the service is easier to do, can be done anywhere, using the applications via the customer's mobile phone, and is easy to operate. Especially during the Covid-19 pandemic, where people are limited to travel and must stay at home, digital wallet users can make all transactions without coming to a counter and without physical touch. The spread of Covid-19 and related government lockdowns increases the rate of finance app downloads (Fu & Mishra, 2022).

The use of digital wallets offers many benefits that support the current digital economy, but it also poses risks for its users. Users have different attitudes and behaviors in dealing with risks. There were phenomena considered the risk for users, such as unpaid balances and failed transfers. The other common problems or risks faced by the users are: the balance is cut off, blocked for no reason, failure to respond, failed cash withdrawals, truncated balances, difficulty in updating data, transactions that cannot be conducted, promised refunds, an error, successful top-up but the balance didn't come in. These make users disappointed and complain through various digital media, such as consumer media, online, and offline media. This dissatisfaction will affect the product image for the user, negative electronic word-of-mouth (Talwar et al., 2021), and even brand hate (Kucuk, 2018).

Recent studies on digital wallets focused more on factors that influence their adoption, which is influenced by habits, performance expectations, trust, and facilitating conditions (Widodo et al., 2019). At the same time, the intention to recommend is driven by aspects of comparative advantage, compatibility, complexity, and observability (Kaur et al., 2020). The next developments in the digital wallet are cryptocurrency wallet (Sung, 2021) and Pure Wallet, which extends the concept of Blockchain cryptocurrency for offline transactions (Igboanusi et al., 2021).

The research gap in this study is the limited number of studies (Müller-Bloch & Kranz, 2015; Robinson et al., 2011) in analyzing the perceived risk-based

segmentation of digital wallet customers. As we all know that market segmentation is essential for business success but the study of customer segmentation by their perceived risk on digital wallets is still limited (Hajibaba et al., 2019). Segmentation provides a good understanding of customer needs and helps identify the company's potential customers (Christy et al., 2021). Customer segmentation is essential for designing marketing campaigns to increase business and revenue (Qadadeh & Abdallah, 2018). A study on customer segmentation is needed to determine who will be served and how to serve their needs and wants based on their respective characteristics. Perceived risk in digital payment has gotten attention from scholars, such as privacy risks from cyberattacks and the threat of data misuse, which have emerged and are increasing the complexity of existing global digital ecosystems (Akanfe et al., 2020). Moreover, risk perception plays a vital role in consumer decision-making; therefore, segmenting customers based on risk needs to be conducted. Ideally, marketing managers should group customers according to their perceived risk (Paulssen et al., 2014). Therefore, this study will try to divide customers based on their perceived risk on digital wallets into the specific segment and identify the characteristics of each segment.

Based on these gaps, this study aims to identify and confirm the perceived risk users face in the digital wallet and classify them into more homogeneous groups based on their risk perceptions, also identifying each group's characteristics, propose recommendations for managing risk, and better serve the segment of digital wallet services. The managerial contribution of this study is to map the type and details of perceived risk in digital wallets and serve customers according to these segments. The theoretical contribution of this study offers a classification of risk perceptions as a basis for segmentation. The study identifies that there are levels of perceived risk users face in digital wallets to add to risk literature.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Risk on digital wallet

Recent studies on the perception of risk in digital wallets in the last three years. Table 1 describes digital wallet studies in risk perception.

Table 1
Perceived risk study on digital wallet

Authors	Objective	The role of risk in digital wallets
(Abdulrahaman *et al*., 2018)	Assessing vulnerabilities in digital wallet transactions and performing risk management empirically to obtain the level of security priority required to ensure the security and privacy of mobile wallet platform users	The login to the digital wallet is the most critical piece of customer information that must be protected. There are vulnerabilities from mobile wallet users that also threaten the security of payment systems and customer transactions that need to be appropriately handled.

Authors	Objective	The role of risk in digital wallets
(Alaeddin *et al*., 2018)	Analyzing attitudes and intentions on traditional payments using paper money, debit or credit cards to digital wallets using mobile applications.	Perceived risk fully moderates the relationship between behavioral attitudes and behavioral intentions to switch to a digital wallet.
(Chakraborty & Mitra, 2018)	Identifying the parameters that are most important in predicting consumer adoption intentions of digital wallets and whether the market can be segmented into different customer groups	Perceived risk does not affect adoption. There are three segments, where the first segment is very concerned about risk, while the second and third segments are less concerned about risk.
(Widodo *et al*., 2019)	Identifying the factors that influence the adoption of digital wallets in Indonesia.	Perceived risk in digital wallet adoption does not affect behavioral intention to adopt digital wallets.
(Aji *et al.*, 2020)	Examining the effect of perceived risk, government support, and perceived benefits on customer intention to use e-wallets during the Covid-19 outbreak in two countries.	Perceived risk affects government support and perceived benefits on customer intentions. The effects of perceived risk and perceived benefit on intention are not different between Indonesia and Malaysia
(Tam, 2012)	Analyzing the barriers to innovation adoption in digital wallets through the lens of innovation resistance theory.	The risk barrier affects the resistance to digital wallet innovation.
(Ming *et al*., 2020)	examine the factors that influence the adoption of E-wallet services in Sarawak	The risk perceived by the user may discontinue the use of the digital wallet.
(Singh *et al*., 2020)	Determining the most significant factors influencing user intentions, perceived satisfaction, and recommendations for using digital wallets	The risk was not found to play a significant role in predicting user intentions to use mobile payment services.
(Nuryasman & Warningsih, 2021)	Examining the effect of perceived benefits, perceived risks, and trust on digital wallet usage intentions among college students	Perceived risk does not affect the intention to use a digital wallet.
(Pham *et al*., 2021)	Examining the impact of perceived risk and perceived value on the use of the Momo e-wallet on users aged 18 to 35 years in Hanoi city.	Perceived value positively influences the intention to use a digital wallet, but the perceived risk is not.
(Undale *et al*., 2021)	Analyzing the influence of demographics (gender and income) on "security concerns" in the use of eWallet during the Covid-19 pandemic situation	Female users pay more attention to e-Wallet security than males do. Middle-income groups are more concerned about the security of digital payments than people from low-income groups are.

Based on this description, a few factors can be found in digital wallets studies such as; first, that risk perception studies on digital wallets focus more on the risk aspect as a variable concerning the intention to adopt (Tam, 2012). Second, the findings on the role of risk are still ambiguous between the findings that state influence and do not affect intentions. Third, risk also acts as a moderating factor, particularly in the relationship between attitude and intention to switch (Alaeddin *et al*., 2018). Fourth,

digital wallet studies in the context of mapping to determine groups formed based on risk perceptions are still very limited, especially groupings based on risk perceptions (e.g., Chakraborty & Mitra, 2018). Fifth, differences in the use of digital wallets have been identified based on gender and income (Undale *et al*., 2021). Thus, risk studies in digital wallets have a limited scope and can be developed in future studies.

Risk-based segmentation

The literature discusses risk-based segmentation in a limited way. The description of segmentation associated with risk can be traced in several studies. One of the studies links segments and risk and examines the relationship between quantity and price risk in different segments of financial intermediaries (Allen & Jagtiani, 1997). This study identifies three segments of financial intermediaries, namely institutional depositors, securities companies, and insurance companies, and finds that market segmentation affects the level of systematic institutional risk. The other study on banking introduces a new intelligent customer segmentation process that automates feature engineering, i.e., the process of using banking knowledge to extract features from raw data through data mining techniques. The new approach achieved 91 percent accuracy compared to the classic approach in detecting, identifying, and classifying transactions into appropriate classifications (Khadivizand *et al*., 2020). The system will enable banks to gain better insight into customers and their behavior by detecting risky activity.

Segmentation studies related to risk are also carried out in the context of tourism services, especially in terms of choosing a target market based on benefit segmentation, with risk criteria, where the three segments formed show different risk characteristics, from high, medium, and high (Jang *et al*., 2002). Risk-based segmentation is also carried out in Insurance services, using the K-Means, Two-Steps, and Kohonen technique, which results in five clusters. Risk segmentation serves as a rational approach to risk management from a resource perspective (Hidalgo *et al.*, 2013). Perceived risk was also studied in terms of product class, where perceived risk was lower for search products, medium for experience products, and high for trust products (Girard & Dion, 2010).

Based on the above, the literature's study of market segmentation related to risk is still limited. In addition, the study does not directly use perceived risk as the basis for segmentation so the segmentation can become a differentiator in influencing the level of risk (Allen & Jagtiani, 1997) and finally becomes a means of detecting risky activities (Khadivizand *et al*., 2020).

RESEARCH METHOD

This research focused on the users of digital wallet services in Indonesia, namely Ovo, Gopay, and Dana. This study used a purposive sampling method, an

unrestricted non-probabilistic sampling method (Cooper & Schindler, 2014), in which sample members were selected because they had criteria that match the set standards. The criteria used in obtaining the sample were: the primary mobile payment users aged over 17 years and using a digital wallet (Ovo, Gopay, and Dana) at least once in the last month.

The source of data in this study is primary data, namely data obtained from respondents. Primary data sources are the most reliable because other parties have not interpreted the information obtained for other purposes (Cooper & Schindler, 2014). A communication approach was used to collect data by questioning and recording their responses for analysis. This approach is often called the survey method or direct questioning technique. In conducting the survey, the researcher used a mail survey technique via a google form due to health reasons (there was still a pandemic so the data gathering process could not be held in person). Data collection was carried out by sending the questionnaire link to a group on WhatsApp, Facebook, and email to prospective respondents from November to December 2020.

This study used nine stages in developing the instrument: identifying information needed, determining the type of interview method, designing questions that allow respondents to be willing and able to answer questions, determining structure, word selection, order, form, and layout, and finalizing and testing the questionnaire (Kahle & Malhotra, 1994). Stages of testing were carried out to obtain measurements that meet the quality of validity - construct, face, and content - and reliability (Trochim et al., 2016). Validity testing was done by ensuring the measurement in the instrument is based on previous studies, peer review opinions, and user opinions. Statistical testing of the instrument was carried out on a small sample involving 30 respondents and revised instrument to become the final instrument.

The measurement and operationalization of constructs or operational definitions (Trochim et al., 2016) used in this study used items from previous studies, which are perceptions of security, financial, social, and operational risks (Lee, 2009; Ryu, 2018). The overall construct was measured by a Likert scale that ranged from "strongly disagree" (1) to "strongly agree" (7). A higher score means a higher level of risk the user perceives (Table 2). It consists of a score of one (very low), two (moderately low), three (slightly low), four (moderate), five (slightly-high), six (moderately high), and seven (very high).

Table 2
Perceived risk level distribution

Interval score	Response	Score	Perceived Risk Level
$1 \leq \times \leq 1.86$	strongly disagree	1	very low
$1.86 < \times \leq 2.72$	disagree	2	low
$2.72 < \times \leq 3.58$	slightly disagree	3	slightly-low
$3.58 < \times \leq 4.44$	neutral	4	moderate
$4.44 < \times \leq 5.3$	slightly agree	5	Slightly-high
$5.3 < \times \leq 6.1$	agree	6	high
$6.1 < \times \leq 7$	strongly agree	7	very high

ANALYSIS AND DISCUSSION

Research Sample

This study involved 270 digital wallet users, of which women (77 percent) dominated the sample, compared to men (23 percent). Most of them are users of OVO (45 percent), Gopay (26 percent), and Dana (29 percent). In terms of age, the most respondents were 21-30 years old (60.7 percent), 17-20 years old (37.8 percent), and the smallest were 21-30 years old (0.7 percent) and over 41 years old (0.7 percent). Respondents who are still students dominate the research sample, followed by employees, others, and entrepreneurs. Regarding the frequency of using digital wallets in one month, most respondents used them once, 2-3 times, and 4 to 5 times. Those who used it more than ten times were 10.4 percent. Because most of the respondents are young students, therefore the respondents of this study can represent young users.

Descriptive analysis

Table 2 shows the responses of the sample in the study. Responses ranged from the highest score (the financial loss of DW applications may occur due to lack of information exchange, 3.99) to the lowest (I am worried that if I do not use the DW application, my family will comment negatively; 2.24). At the same time, the standard deviation ranged from the highest (I am afraid my friends will laugh at me for not using the DW application, 1.80) to the lowest (the response of DW application providers is slow when financial losses occur, 1.23). This score shows the diversity of respondents' answers to the study items.

Factor Analysis

Factor analysis was carried out by following seven stages, which are: determining goals, designing factor analysis, determining assumptions, obtaining factors and measuring overall conformity, factor interpretation, validation, and data reduction (Hair et al., 2018). The unit of analysis used was the variable (R factor analysis). All data used was matrix data, in which the number of samples was 270 or has met the minimum number limit (100 observations). The data feasibility check was carried out before conducting the factor analysis. Regarding the adequacy of inter-correlation between data or testing the correlation between items, the study found the correlation between items was more than 60% through Pearson correlation. This result shows a significant correlation between items. Bartlett's sphericity test shows sufficient correlation in the factors so that factor analysis could be or was feasible (chi-square = 2.62E+03, df: 105, p = 0.000). While the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (MSA) shows a value of 0.794 which means it was quite good or had met the cut-off value (MSA> 0.5) (Hair et al., 2018). Thus, the data has met the requirements, and factor analysis could be performed.

Factor analysis was performed using principal components for extraction and varimax for rotation methods. The purpose of rotation of the factor loading matrix is

to facilitate interpretation so that each factor is associated with a small block of observed variables (Acal et al., 2020). This study used a combination of theoretical and empirical evidence to determine the number of factors. Some of the stopping criteria to determine the number of factors were: the previous study, the eigenvalue of more than 1, and variance explained exceeding 60 percent. Previous studies tend to focus on four factors (Lee, 2009; Ryu, 2018). The estimation of factor analysis resulted in four factors with eigenvalues of 5,427 (factor 1), 2,602 (factor 2), 1,730 (factor 3), and 1,352 (factor 4). The variance explained was 74.03. The results of the factor analysis are as in Table 2.

Table 3
Means, standard deviation, loading, and risk factors

Items	Mean	Std. Deviation	Loading Factor	Risk Factors (α/ Eigenvalue) (Mean /Risk level)
There is a potential risk in payments using the DW application	3.40	1.51	0.776	Factor 1: Security Risk (0.89/5.43) (3.4/slightly-low)
There is a potential risk in processing payment transactions with the DW application	3.44	1.56	0.809	
User authentication on the DW application is not secure	2.87	1.35	0.776	
Transactions authentication in the DW application is not secure	2.89	1.32	0.769	
I'm worried about the misuse of my financial information when using the DW application	3.64	1.70	0.799	
I am worried that an unauthorized person may access the DW application's financial information.	3.96	1.79	0.804	
When using the DW application, there is a possibility of financial loss.	3.53	1.73	0.822	Factor 2: Financial Risk (0.83/2.60) (3.7/moderate)
Cheating in payments may occur when using the DW application.	3.57	1.64	0.771	
The financial loss of the DW application may occur due to a lack of information exchange.	3.99	1.57	0.720	
I am worried that my family will comment negatively if I do not use the DW application.	2.24	1.55	0.851	Factor 3: Social Risk (0.90/1.73) (2.4/ low)
I am worried that my family will think I am outdated if I do not use the DW mobile payment application.	2.40	1.70	0.919	
I am worried that my friends will laugh at me for not using the DW application.	2.60	1.80	0.896	
The DW application provider does not want to solve the problem if I experience a financial loss.	3.37	1.46	0.732	Factor 4: Operational Risk (0.78/1.35) (3.5/slightly-low)
The response of DW application providers is slow when financial losses occur.	3.44	1.23	0.794	
If a financial loss occurs, I am worried about how the DW provider resolves it.	3.77	1.36	0.781	

Note: DW= Digital Wallet

Table 3 shows that the perceived risk of digital payment consists of four factors: security, financial, social, and operational risk. Security risk is uncertainty reflected in six indicators, where the most dominants are the risk of payment transactions (0.809), and the risk of unauthorized people can access financial information (0.804). Financial risk consists of three leading indicators, and which risk of financial losses (0.822) was the most important. Social risk compose three indicators, where the risk of families thinking outdated when not using the digital wallet (0.919) was the most dominant. Meanwhile, operational risk includes three indicators, and the dominant indicator of providers is slowly responding to financial losses (0.794).

Cluster Analysis

Cluster analysis defines the data structure by placing the most similar observations into groups. There were three steps in performing cluster analysis: determining similarity measurements, forming clusters, and determining how many clusters (Hair et al., 2018). This study used the partition procedure by nonhierarchical procedure because samples were below 300 and generally less sensitive to outliers. The statistical algorithm used the K-means algorithm by partitioning data into a predetermined number of clusters and iteratively reassigning observations to groups until several numerical criteria were met. K-means algorithm is the most commonly used due to the simple clustering method (Yu et al., 2018). In determining the number of clusters, it was used theoretical validation approach was assessed through external validation. The polarization cluster in the literature shows a stratified risk pattern, namely high, medium, and low (e.g., Girard & Dion, 2010; Jang et al., 2002). The results of cluster analysis are shown in Table 4.

Table 4
Cluster Center

Risk factors	Cluster 1 (49%)	Cluster 2 (4%)	Cluster 3 (47%)
Security risk	-0.068	0.714	0.008
Financial risk	-0.433	1.679	0.299
Social risk	0.573	2.081	-0.765
Operational risk	0.409	-2.181	-0.231

The cluster validation was carried out by ANOVA analysis, and it looks at the cluster differences based on perceived risk factors. The results of this different test are in Table 4.

Table 5
Description of ANOVA in each cluster

Risk Factor	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
Security risk	3.105	2	0.984	267	3.154	0.044
Financial risk	33.471	2	0.757	267	44.228	0.000
Social risk	82.747	2	0.388	267	213.45	0.000
Operational risk	40.524	2	0.704	267	57.568	0.000

Based on the mean difference test, the table showed the differences among clusters: security risk (p=0.044), financial risk (p=0.000), social risk (p=0.000), and operational risk (p=0.000). These results confirm that four perceived risk factors were different between the clusters.

Table 6
Segment risk perception profile (Average score and ANOVA test)

Risk and indicators	Mean (Risk Level)			Anova	
	MRS (49%)	HRS (4%)	LRS (47%)	F	Sig.
Security risk	3.4	4.6	3.3	-	-
Potential risk in payments	3.5	6.1	3.1	24.647	0.00
Potential risks in the transaction process	3.5	5.6	3.2	13.183	0.00
User authentication security	2.8	1.7	3.0	4.718	0.01
Proof of authenticity of unsafe transactions	3.0	1.7	2.9	4.618	0.01
Misuse of financial information	3.7	6.2	3.4	14.844	0.00
Access financial information from others	3.9	6.1	3.8	8.726	0.00
Financial risk	4.5	6.0	2.7	-	-
Possible financial loss	4.4	5.9	2.4	94.698	0.00
Cheating in payments	4.3	6.1	2.6	72.000	0.00
Application financial loss	4.8	5.9	3.1	68.627	0.00
Social risk	2.1	5.2	2.6	-	-
family comment negatively	2.0	5.0	2.3	21.686	0.00
family think outdated	1.9	5.0	2.7	23.561	0.00
friends laughed	2.2	5.5	2.8	20.178	0.00
Operational risk	4.1	2.4	3.1	-	-
The provider doesn't want to solve the problem	3.8	2.1	3.1	13.567	0.00
Slow response of providers	4.0	2.4	3.0	28.236	0.00
The way the provider solves a problem	4.4	2.6	3.2	34.798	0.00

Note : MRS: Medium-risk segment; HRS; High-risk segment; LRS; Low-risk segment.

Based on the cluster center, this study identifies the cluster characteristics based on the mean score of perceived risk in each cluster (Table 7). The cluster analysis results show three clusters with characteristics described by the scores of their perceived risk. Figure 1 shows the cluster perceived risk scores ranged from the lowest in the second cluster (2.1) to the highest in the first cluster (6.0). High or low scores indicate high or low user attention to certain perceived risk factors. Based on these characteristics, we name the groups based on risk hierarchy, namely cluster 1 as the medium-risk segment (MRS), cluster 2 as the high-risk segment (HRS), and Cluster 3 as the low-risk segment (LRS). MRS was characterized by slightly low levels of a security risk (3.4), slightly high financial risk (4.5), moderately low social risk (2.1), and moderate operational risk (4.1). The highest score characterized HRS compared to other clusters, such as slightly high on security (4.6), moderately high on financial risk (6.0), slightly high on social risks (5.2), but the lowest score among the clusters, namely slightly low on operational risks (2.4). In comparison, LRS was indicated as slightly low on security risk (3.3), moderately low on financial risk (2.7) and operational risk (2.6), and slightly low on social risk (3.1).

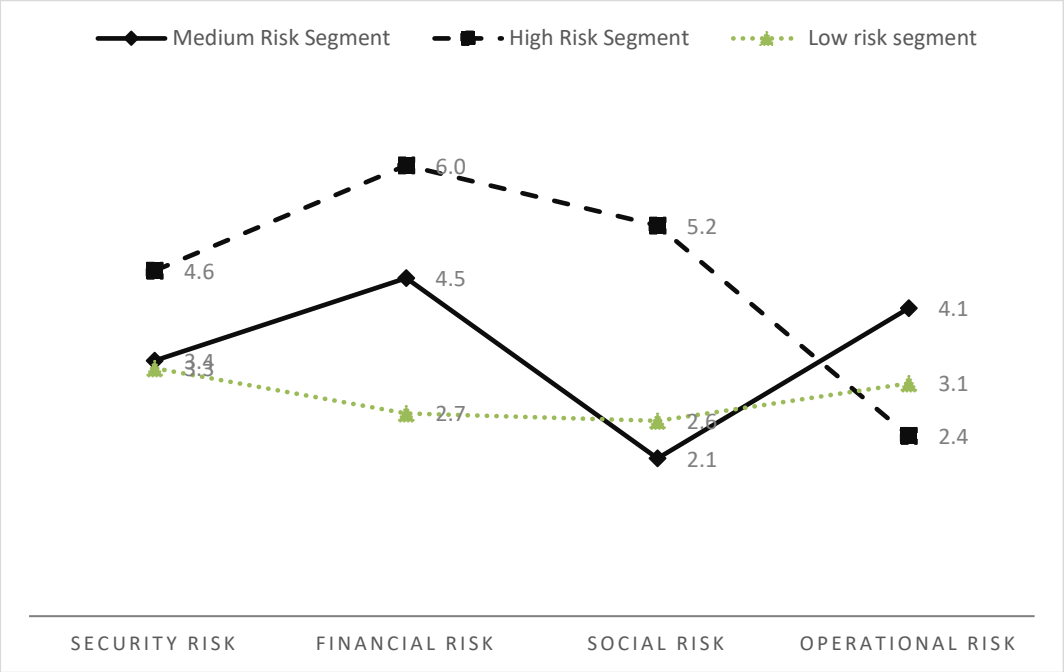

Figure 1
Mean Custer Comparison

The segment profile based on perceived risk is described in Table 7. The high-risk segment appears to have a higher sensitivity to almost all risks except operational risk. On security risk, this segment is the most sensitive to risk in payments, misuse of financial information, and possible access of an unauthorized person to financial data, even though this segment is the least susceptible to user and transaction authentication. Financial risk is the most sensitive among other clusters, such as financial loss and cheating. In addition, on social risks, they were the most sensitive segment among groups, while in terms of operational risk indicators, they are the least sensitive. The medium-risk segment is characterized by moderate sensitivity to almost all security and financial risk indicators, except they are the most sensitive to user authentication risk. However, this segment is the lowest on social risk indicators and the highest on operational risk indicators. The low-risk segment has the lowest risk sensitivity, especially in almost all security risk indicators, except for the risk of authenticating users and transactions. This segment also has the lowest sensitivity on all financial risk indicators; however, this segment has moderate risk sensitivity on social and operational risk indicators. The mean difference test in these three segments on risk perception indicates a significant difference level ($p < 0.05$).

Segment profile

There are three segments of digital wallets based on their perceived risk. The largest size of the segment is the medium-risk segment (49 percent), followed by the low-risk segment (47 percent) and the high-risk segment (4 percent). Table 7. shows

the segment profile based on demographic aspects.

Table 7
Demographic profile of perceived risk segments (percentage)

Category	Sub-category	MRS (%)	HRS (%)	LRS (%)	Total (%)
Sex	Male	23	64	20	23
	Female	77	36	80	77
Ages (year)	17-20	38	46	36	38
	21-30	60	54	62	61
	> 31	2	0	1	1
Job	Employee	14	0	8	11
	Entrepreneur	4	0	1	2
	Student	77	82	85	81
	Others	5	18	6	6
Frequency of use in one month (times)	1	31	0	32	30
	2-3	27	9	28	27
	4-5	25	9	23	23
	6-7	7	0	5	6
	8-9	2	9	5	4
	≥10	8	73	7	10
Digital payment	OVO	49	0	46	45
	Gopay	25	9	28	26
	Dana	26	91	26	29
Total		100	100	100	100

Note : MRS: Medium-risk segment; HRS; High-risk segment; LRS; Low-risk segment

By gender, females dominate the medium-risk segment (77 percent) and low-risk segment (80 percent), while males dominate the high-risk segment (64 percent). In terms of age, ages 21-30 are salient in the medium-risk segment (60 percent), high-risk segment (54 percent), and low-risk segment (61 percent). Based on occupations, students dominate all three clusters. From the frequency of mobile payment, most users use digital wallets as much as 1-7 times a month, except for the high-risk segment (91 percent) that uses ten times or more. While from digital wallet types, most of them used the Dana, except for the high-risk segment. This result indicates that the high-risk segment is the highest frequency in digital wallets, mainly the Dana application.

Digital wallet risk perception factors

The critical finding of this study is confirmation of the types of risks perceived by digital wallet users during the Covid-19 pandemic. There were four risks: security, financial, social, and operational risks. The level of the risk is slightly low, with which the highest level is on financial risk, and the lowest is on social risk.

Security risk describes uncertainty perceived by digital wallet users regarding potential risks during payments, transaction processing, user and transaction authentication, and misuse and unauthorized access to financial information. Security risk is on a slightly low level. In particular, the highest level is the risk of abuse and unauthorized people accessing financial information. The lowest level of security risk is for authenticating users and transactions. These findings are consistent with previous studies, which stated that login details are the most important and require the most

protection (Abdulrahaman *et al*., 2018). The security aspect is also a significant predictor of the adoption of digital payments (Alkhowaiter, 2020).

Financial risk indicates uncertainty for the potential risk of financial losses, cheating in payments, and financial losses due to lack of information exchange. Financial risk is at a moderate level of risk, which this risk is the highest level of risk among digital wallets risks. Financial losses due to lack of exchanging information were the most important for the user, followed by cheating in payments and financial loss when using the application. Perceived financial risk affects behavioral intention (Quan *et al*., 2022) and customer authentication (Lee *et al.*, 2012).

Social risk refers to the risks of not using the digital wallet family will comment negatively or be outdated, and friends will laugh. The social risk was the lowest level among digital wallet risks. Ancient comments from family were the most important for a user. These findings confirm previous studies that significant social influence can reduce users' perceived satisfaction, further affecting user recommendations for using services in digital wallets (Singh *et al*., 2020).

Operational risk describes the provider's unwillingness to solve problems, slow response, and how the provider solves problems when a loss occurs. In general, the level of operational risk is slightly low. How providers solve problems when a financial loss occurs was the most important to be perceived by digital wallet users.

Digital wallet user segment

Another important finding of this study is that there were three digital wallet customer segments based on perceived security, financial, social, and operational risks: high, medium, and low risk. From the size of a sample, the moderate-risk segment is the majority; however, the high-risk segment is a minority.

High-risk segment. This segment represents four percent of the sample. It was the most sensitive to security, financial, and social risk; however, it was the least sensitive to operational risk. The high-risk level includes misuse of financial information, unauthorized people accessing financial information, risk in payment, and cheating. Even though they perceive authenticating users and transactions as shallow risk, compared to other segments, this segment also perceived financial risk level as the highest. Social risk for this segment is also perceived as slightly high risk. Moreover, their operational risk is low-level, even the lowest compared to other segments. Even though their proportion is small, they were a group of users frequently using a digital wallet. In the literature, customers who perceive high risk will influence their behavior related to the provider (Cambra-Fierro *et al*., 2018) and will minimize risk. To do so, they are likely to choose another provider (Tzavlopoulos *et al.*, 2019).

Medium-risk segment. This segment represents 49 percent of the sample or the majority. It was the least sensitive segment to security and financial risks; however, they were the most susceptible to operational risk. This segment was as moderately

sensitive to social risks. For them, the highest perceived risk was a security risk, particularly concerning the misuse of information and unauthorized people can access financial information, even though the risk status was moderate. This segment also perceived that the level of financial risk is moderate. They perceived social risk as low risk and operational risk as medium risk. Even operational risk was the highest compared to other segments. Therefore, most of this segment considers the risk to digital wallets moderate.

Low-risk segment. This segment represents 47 percent of the sample. This segment perceived security and financial risks as the lowest, meaning they were the least sensitive to this risk. This segment perceived social and operational risk as moderate compared to other segments. However, the surprising finding was that the risk of authentication in this segment has the highest level compared to different segments, even though the perceived risk category level is relatively low. Thus, this confirms again that some digital wallet users feel that the perceived risk is low. These customer segments need to be considered because there are differences in attitudes towards high and low-risk perceptions. Customers with high risk who feel satisfied are more likely to revisit than those with low risk (Tam, 2012); also, satisfaction on loyalty will be weaker in consumers who perceive higher risk (Tuu *et al*., 2011). Regarding the relationship process, the effectiveness of social bonding tactics as a determinant of trust depends on risk perception. When the risk is low, satisfaction determines loyalty, while when risk is low, it does not determine loyalty.

CONCLUSION AND SUGGESTIONS

Perceived risks in digital wallets could be classified into four factors: security, financial, social, and operational risks. These risks confirmed the perceived risk of other services in the literature. The highest level of perceived risk was a financial risk, while the lowest was a social risk. In general, the level of perceived risk is slightly low. The three highest indicators of perceived risk were the risk of financial loss, the risk of unauthorized person may able to access financial information, and the way provider solves financial loss problem.

Digital wallet users were grouped into three segments based on their perceived risk: high, medium, and low-risk. The three segments have different characteristics. The high-risk segment stands out for its high sensitivity to social, financial, and security risks, where they pay the slightest attention to operational risk. The moderate-risk segment pays more attention to operational and social risks but at least pays attention to two other risks, security and financial. This segment has the highest elasticity in terms of operational risk. The low-risk segment were users who considered social and operational risks less and less about financial and security risks.

This study tries to close the gap of the absence of risk-based customer segmentation in digital wallets and found a description of digital wallet customers

based on risk. Therefore, this study adds to the literature on the segments formed in digital wallet services.

The crucial managerial implication of this study is how to manage the perceived risks of digital wallet users and how to serve risk-based segments by considering their risk perception, demographic characteristics, and limitation of this study. The perceived risks of digital wallet users are at a slightly low level. Nevertheless, digital wallet service management needs to pay attention to and mitigate the risks to reduce negative perceptions of using a digital wallet.

On security risks, the critical step to mitigate risk is focused on the risk of financial loss in processing payment transactions and the risk of an unauthorized person accessing the user's financial information. For a user, this risk is essential; therefore, users consider this risk when using a digital wallet. Regarding financial risk, digital wallet management needs to mitigate the risk of possible financial loss when using the application. The social risk that needs to be mitigated is the risk of outdated thinking from family, which is an essential social risk, even though the perceived level of risk is low. In the mitigation of operational risks, the most critical risk is a slow response from the provider, even with a low-moderate level of the risk. Thus, even if the level of risk is low-moderate, the perceived risk of using digital wallets needs to be mitigated. Risk mitigation can be performed by developing an acceptable use and security policy, routinely monitoring the digital wallet system, monitoring employee internet activity, user education and training programs, software updates, archiving digital wallet transactions, and developing warning and response plans for transactions incidents (He, 2012).

Managing high-risk segment. Management in the high segment can be done by paying more attention to the perceived risks. In general, mitigation steps can be conducted by developing a clear policy on their perceived risk. Moreover, it needs to educate through social media or applications regarding preventing the misuse of information, the possibility of others accessing information, and financial risks during payments. Finally, developing a plan to respond quickly complaint to the risk is essential (Stevens et al., 2018).

Managing medium-risk segment. Working in this segment means paying more attention to operational risk mitigation because this is the most perceived. This risk mainly reduces user concerns about how providers solve problems, even if the risk to them is medium-low. In addition, this is related to the anticipation of the provider to respond quickly to user complaints if the user is exposed to adverse problems. Digital wallet providers also need to demonstrate a desire to resolve issues so that users can be confident that the provider will decide their issues if they occur.

Managing low-risk segment. The low-risk segment requires mitigating social and operational risk because this segment feels this risk. Although relatively low, these two risks for this segment need anticipation, especially in service providers' desire,

method, and response to problem-solving. Communication regarding this matter properly will maintain the perception that this risk is relatively low or even low. Worries about the possibility of others accessing financial information are also the most perceived risk for this segment, so providers need to communicate and ensure this does not happen.

The study is not without limitations. The first is the current sampling technique limits the findings to be generalized; therefore, it recommends that further research use random sampling. Second, this study's risk type ignores psychological and time risks. Future studies are expected to identify more complete risk dimensions, such as a resource perspective (Hidalgo et al., 2013), product class (Girard & Dion, 2010), and intelligent-risk based (Khadivizand et al., 2020). Third, this study is limited in identifying risk from dimensionality in identifying the risk-based segments but has not identified the role of risk in the context of other marketing interests, such as marketing performance. Further studies are recommended to analyze each segment's role concerning the value and intention to reuse (Filho et al., 2020).

REFERENCES

Abdulrahaman, M. D., Alhassan, J. K., Ojeniyi, J. A., & Abdulhamid, S. M. (2018). Security risk analysis and management in mobile wallet transaction: A case study of Pagatech Nigeria Limited. *International Journal of Computer Network and Information Security, 10*(12), 21–33. https://doi.org/10.5815/ijcnis.2018.12.03

Acal, C., Aguilera, A. M., & Escabias, M. (2020). New modeling approaches based on varimax rotation of functional principal components. *Mathematics*, *8*(11), 1–15. https://doi.org/10.3390/math8112085

Aji, H. M., Berakon, I., & Husin, M. M. (2020). Covid-19 and e-wallet usage intention: A multigroup analysis between Indonesia and Malaysia. *Cogent Business & Management*, *7*(1), 1–15. https://doi.org/10.1080/23311975.2020.1804181

Akanfe, O., Valecha, R., & Rao, H. R. (2020). Assessing country-level privacy risk for digital payment systems. *Computers & Security*, *99*, 102065. https://doi.org/10.1016/j.cose.2020.102065

Alaeddin, O., Altounjy, R., Zainudin, Z., & Kamarudin, F. (2018). From physical to digital: Investigating consumer behaviour of switching to mobile wallet. *Polish Journal of Management Studies, 17*(2), 18–30. https://doi.org/10.17512/pjms.2018.17.2.02

Alkhowaiter, W. A. (2020). Digital payment and banking adoption research in Gulf countries: A systematic literature review. *International Journal of Information Management*, *53*, 102102. https://doi.org/10.1016/j.ijinfomgt.2020.102102

Allen, L., & Jagtiani, J. (1997). Risk and market segmentation in financial intermediaries' returns. *Journal of Financial Services Research, 12*(2–3), 159–173. https://doi.org/10.1023/A:1007974719557

Cambra-Fierro, J., Melero-Polo, I., Sese, F. J., & van Doorn, J. (2018). Customer-firm interactions and the path to profitability. *Journal of Service Research, 21*(2), 201–218. https://doi.org/10.1177/1094670517738369

Chakraborty, S., & Mitra, D. (2018). A study on consumers adoption intention for digital wallets in India. *International Journal on Customer Relations*, *6*(1), 38–57.

Christy, A. J., Umamakeswari, A., Priyatharsini, L., & Neyaa, A. (2021). RFM ranking – An effective approach to customer segmentation. *Journal of King Saud University - Computer and Information Sciences*, *33*(10), 1251–1257. https://doi.org/10.1016/j.jksuci.2018.09.004

Cooper, D. R., & Schindler, P. S. (2014). *Bussiness research methods*. Boston: McGraw-Hill Irwin.

Filho, E. J. M. A., Simões, J. D. S., & De Muylder, C. F. (2020). The low effect of perceived risk in the relation between hedonic values and purchase intention. *Journal of Marketing Management*, *36*(1–2), 128–148. https://doi.org/10.1080/0267257X.2019.1697725

Fu, J., & Mishra, M. (2022). Fintech in the time of Covid-19: Technological adoption during crises. *Journal of Financial Intermediation*, *50*, 100945. https://doi.org/10.1016/j.jfi.2021.100945

Girard, T., & Dion, P. (2010). Validating the search, experience, and credence product classification framework. *Journal of Business Research*, *63*(9–10), 1079–1087. https://doi.org/10.1016/j.jbusres.2008.12.011

Hair, J. F. J., Black, W. C., Babin, B. J., Anderson, R. E., Black, W. C., & Anderson, R. E. (2018). *Multivariate data analysis* (pp. 95–120). https://doi.org/10.1002/9781119409137.ch4

Hajibaba, H., Grün, B., & Dolnicar, S. (2019). Improving the stability of market segmentation analysis. *International Journal of Contemporary Hospitality Management*, *32*(4), 1393–1411. https://doi.org/10.1108/IJCHM-02-2019-0137

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*, *14*(2), 171–180. https://doi.org/10.1108/13287261211232180

Hidalgo, H., Chipulu, M., & Ojiako, U. (2013). Risk segmentation in Chilean social health insurance. *International Journal of Health Care Quality Assurance*, *26*(7), 666–681. https://doi.org/10.1108/IJHCQA-05-2012-0045

Igboanusi, I. S., Dirgantoro, K. P., Lee, J.-M., & Kim, D.-S. (2021). Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture. *ICT Express*, *7*(3), 327–334. https://doi.org/10.1016/j.icte.2021.08.004

Jang, S. C., Morrison, A. M., & O'Leary, J. T. (2002). Benefit segmentation of Japanese pleasure travelers to the USA and Canada: Selecting target markets based on the profitability and risk of individual market segments. *Tourism Management*, *23*(4), 367–378. https://doi.org/10.1016/S0261-5177(01)00096-6

Kahle, L. R., & Malhotra, N. K. (1994). Marketing research: An applied orientation. *Journal of Marketing Research*, *31*(1), 137. https://doi.org/10.2307/3151953

Kaur, P., Dhir, A., Bodhi, R., Singh, T., & Almotairi, M. (2020). Why do people use and recommend m-wallets? *Journal of Retailing and Consumer Services*, *56*, 102091. https://doi.org/10.1016/j.jretconser.2020.102091

Khadivizand, S., Beheshti, A., Sobhanmanesh, F., Sheng, Q. Z., Istanbouli, E., Wood, S., & Pezaro, D. (2020). Towards intelligent feature engineering for risk-based customer segmentation in banking. *Proceedings of the 18th International Conference on Advances in Mobile Computing & Multimedia*, 74–83. https://doi.org/10.1145/3428690.3429172

Kucuk, S. U. (2018). Macro-level antecedents of consumer brand hate. *Journal of Consumer Marketing*, *35*(5), 555–564. https://doi.org/10.1108/JCM-10-2017-2389

Lee, J.-E. R., Rao, S., Nass, C., Forssell, K., & John, J. M. (2012). When do online shoppers appreciate security enhancement efforts? Effects of financial risk and security level on evaluations of customer authentication. *International Journal of Human-Computer Studies*, *70*(5), 364–376. https://doi.org/10.1016/j.ijhcs.2011.12.002

Lee, M. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, *8*(3), 130–141. https://doi.org/10.1016/j.elerap.2008.11.006

Ming, K. L. Y., Jais, M., Wen, C. C., & Zaidi, N. S. (2020). Factor affecting adoption of E-wallet in Sarawak. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *10*(2), 244–256. https://doi.org/10.6007/IJARAFMS/v10-i2/7446

Müller-Bloch, C., & Kranz, J. (2015). A framework for rigorously identifying research gaps in qualitative literature reviews. *Proceedings of the 36th International Conference on Information Systems (ICIS)*, 1–19.

Nuryasman, M., & Warningsih, S. (2021). Determining factors of digital wallet usage.

Jurnal Manajemen, *25*(2), 271–289. https://doi.org/10.24912/jm.v25i2.740

Paulssen, M., Roulet, R., & Wilke, S. (2014). Risk as moderator of the trust-loyalty relationship. *European Journal of Marketing*, *48*(5/6), 964–981. https://doi.org/10.1108/EJM-11-2011-0657

Pham, V. T., Dung, D. Van, Mai, P. V. N., Anh, T. N., & Anh, H. D. (2021). Effect of perceived risk, perceived value to intention to use Momo e-wallet. *Gyanshauryam International Scientific Refereed Research Journal*, *4*(2), 50–60. https://doi.org/10.32628/GISRRJ21327

Qadadeh, W., & Abdallah, S. (2018). Customers segmentation in the insurance company (TIC) dataset. *Procedia Computer Science*, *144*, 277–290. https://doi.org/10.1016/j.procs.2018.10.529

Quan, L., Al-Ansi, A., & Han, H. (2022). Assessing customer financial risk perception and attitude in the hotel industry: Exploring the role of protective measures against Covid-19. *International Journal of Hospitality Management*, *101*(July 2021), 103123. https://doi.org/10.1016/j.ijhm.2021.103123

Robinson, K. A., Saldanha, I. J., & Mckoy, N. A. (2011). Development of a framework to identify research gaps from systematic reviews. *Journal of Clinical Epidemiology*, *64*(12), 1325–1330. https://doi.org/10.1016/j.jclinepi.2011.06.009

Ryu, H.-S. (2018). What makes users willing or hesitant to use fintech? The moderating effect of user type. *Industrial Management & Data Systems*, *118*(3), 541–569. https://doi.org/10.1108/IMDS-07-2017-0325

Singh, N., Sinha, N., & Liébana-Cabanillas, F. J. (2020). Determining factors in the adoption and recommendation of mobile wallet services in India: Analysis of the effect of innovativeness, stress to use and social influence. *International Journal of Information Management*, *50*(May 2019), 191–205. https://doi.org/10.1016/j.ijinfomgt.2019.05.022

Stevens, J. L., Spaid, B. I., Breazeale, M., & Jones, C. L. E. (2018). Timeliness, transparency, and trust: A framework for managing online customer complaints. *Business Horizons*, *61*(3), 375–384. https://doi.org/10.1016/j.bushor.2018.01.007

Sung, S. (2021). A new key protocol design for cryptocurrency wallet. *ICT Express*, *7*(3), 316–321. https://doi.org/10.1016/j.icte.2021.08.002

Talwar, M., Talwar, S., Kaur, P., Islam, A. K. M. N., & Dhir, A. (2021). Positive and negative word of mouth (WOM) are not necessarily opposites: A reappraisal using the dual factor theory. *Journal of Retailing and Consumer Services*, *63*(September), 102396. https://doi.org/10.1016/j.jretconser.2020.102396

Tam, J. L. (2012). The moderating role of perceived risk in loyalty intentions: An

investigation in a service context. *Marketing Intelligence & Planning*, *30*(1), 33–52. https://doi.org/10.1108/02634501211193903

Trochim, W. M., Donnelly, J. P., & Arora, K. (2016). *Reasearch methods: The essential knowledge base*. Boston: Cengage Learning.

Tuu, H. H., Olsen, S. O., & Linh, P. T. T. (2011). The moderator effects of perceived risk, objective knowledge and certainty in the satisfaction-loyalty relationship. *Journal of Consumer Marketing*, *28*(5), 363–375. https://doi.org/10.1108/07363761111150017

Tzavlopoulos, I., Gotzamani, K., Andronikidis, A., & Vassiliadis, C. (2019). Determining the impact of e-commerce quality on customers' perceived risk, satisfaction, value and loyalty. *International Journal of Quality and Service Sciences*, *11*(4), 576–587. https://doi.org/10.1108/IJQSS-03-2019-0047

Undale, S., Kulkarni, A., & Patil, H. (2021). Perceived eWallet security: Impact of Covid-19 pandemic. *Vilakshan - XIMB Journal of Management*, *18*(1), 89–104. https://doi.org/10.1108/XJM-07-2020-0022

Widodo, M., Irawan, M. I., & Sukmono, R. A. (2019). Extending UTAUT2 to explore digital wallet adoption in Indonesia. *2019 International Conference on Information and Communications Technology (ICOIACT)*, 878–883. https://doi.org/10.1109/ICOIACT46704.2019.8938415

Yu, S.-S., Chu, S.-W., Wang, C.-M., Chan, Y.-K., & Chang, T.-C. (2018). Two improved k-means algorithms. *Applied Soft Computing*, *68*, 747–755. https://doi.org/10.1016/j.asoc.2017.08.032