BSIJ *Business System & Innovation Journal*
Research • Innovation • Digital Transformation

YAYASAN FATHUR RAHMAN
Vol. 01, Issue 03, 2026 | e-ISSN 3163-2831

Ethical and Privacy Governance Dimensions in the Adoption of Digital Payment Systems in the MSME Sector

Hatta Z[1]*, Jonathan Kurniawan[2]

1 Department of Computer Science, Faculty of Computer Science, Universitas Persada Bunda Indonesia, Pekanbaru, Indonesia
2 Department of Computer Science, Faculty of Computer Science, University of Brawijaya, Malang, Indonesia
* Correspondence: hattaasyaki@gmail.com

OPEN ACCESS
No article processing charge (APC)

ARTICLE INFORMATION

Page
114-129

Received
7 October 2026

Revised
10 October 2026

Accepted
11 October 2026

Published
30 October 2026

DOI
https://doi.org/10.67955/bsij.v1i3.35

Copyright
© 2026 by the author(s). Articles published in this journal are licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0) license, which permits others to copy, distribute, display, and adapt the work, provided that appropriate credit is given to the original authors and to the journal as the first place of publication.

Abstract. The continuous digital transformation among Micro, Small, and Medium Enterprises (MSMEs) has accelerated the adoption of digital payment systems, fundamentally altering not only transactional efficiency but also inducing the profound datafication of commercial activities. This platformization of financial services introduces critical ethical and privacy governance challenges, particularly within the regulatory landscape shaped by Indonesia's Personal Data Protection Law (Law No. 27 of 2022). Consequently, this study aims to investigate how MSME merchants perceive and navigate data privacy issues, identify the accountability challenges embedded in platform-mediated transaction data flows, and explore feasible privacy governance practices tailored to small-scale businesses. Employing an exploratory qualitative case study design, the research analyzes empirical data collected from 15 heterogeneous MSME informants in Pekanbaru, Riau, utilizing a triangulation approach that encompasses semi-structured interviews, operational observations, and document analysis. The thematic analysis reveals a substantial privacy literacy gap, wherein merchants predominantly understand transaction records as mere proof of payment rather than as sensitive information requiring comprehensive lifecycle governance. Furthermore, a significant accountability dilemma emerges due to fragmented responsibilities across merchants and external payment providers, leading to uncertainty regarding data protection obligations. The study also highlights a structural platform dependency that, while functionally beneficial for MSMEs, creates severe informational asymmetries where merchants possess limited influence over downstream data processing practices. In response to these multifaceted challenges, the findings strongly indicate that feasible privacy governance for MSMEs must be proportionate to their limited organizational capacity, heavily favoring simple, routine-integrated controls such as basic access restrictions and data minimization over complex, enterprise-scale compliance bureaucracies. Ultimately, this research theoretically reframes MSME merchants as active organizational privacy actors rather than passive technology users, proposing a proportionate data governance logic that strictly aligns data visibility, ethical responsibility, and platform accountability within the broader digital payment ecosystem.

Keywords: Digital Payment Adoption; MSMEs; Data Privacy Governance; Privacy Literacy; Data Ethics; Platform Accountability

1. Introduction

Digital transformation has progressively altered how micro, small, and medium-sized enterprises (MSMEs) organize sales, customer interaction, financial administration, and payment processes. Digital payment systems have become an increasingly visible component of this transformation because they allow merchants to receive payments through mobile banking, e-wallets, QR-based payment mechanisms, and platform-mediated payment services. In Indonesia, this transformation has moved beyond a peripheral adoption phenomenon. Bank Indonesia reported that by June 2026, QRIS had reached 65.77 million users and 44.86 million merchants, with MSMEs accounting for 96.68% of QRIS merchants. Recent MSME studies similarly indicate that digitalization is associated with organizational adaptation, resilience, and new modes of business-model development rather than simply the acquisition of isolated technologies (Khurana et al., 2022; Skare et al., 2023).

However, the organizational significance of digital payment extends beyond efficiency. A digital payment transaction inherently induces the datafication of commercial activities, creating new informational relationships among customers, merchants, and technology intermediaries (Allen et al., 2021). This platformization of financial services introduces critical privacy challenges regarding what information is collected, who is responsible for it, and how it is shared. In the context of Indonesia's Personal Data Protection Law. the practical challenge for MSMEs is possessing the organizational capability to translate these regulatory obligations into feasible routines for everyday operations (Zhao et al., 2020).

At the merchant level, this transition creates distinct governance tensions: limited privacy literacy, fragmented data responsibility across multiple infrastructural actors, operationally ambiguous consent mechanisms, and severe informational asymmetries between large platforms and small merchants (Suryono et al., 2020). While recent literature extensively examines digital payment adoption through constructs like perceived usefulness and behavioral intention (Ozturk

& Ullah, 2022; Skare et al., 2023), less attention has been given to what adoption means for the governance of transaction-related information after the fact. The intersection between data-governance research and the everyday realities of MSME merchants using platform-mediated payment ecosystems remains comparatively underexplored (Pizzi et al., 2021; Tay et al., 2022).

This study addresses three questions:

RQ1: How do MSME merchants understand and experience data privacy issues in digital payment transactions?

RQ2: What ethical and accountability challenges emerge from the collection and use of transaction-related customer data?

RQ3: How can privacy governance practices be designed to be feasible for small-scale merchants?

The novelty of this study lies in shifting the analytical unit from adoption as an outcome toward post-adoption information governance as a critical organizational problem. By framing MSME merchants as active organizational privacy actors rather than passive technology users, this research integrates digital-payment datafication, ethical responsibility, and governance feasibility into a single qualitative inquiry. The practical contribution is the development of a proportionate governance logic that does not assume MSMEs possess the organizational resources of large enterprises, ensuring data visibility, ethical responsibility, and platform accountability align within the broader digital payment ecosystem.

2. Literature Review and Theoretical Background

2.1. Digital Transformation and MSME Payment Ecosystems

Digital transformation in MSMEs is better understood as organizational change enabled by digital technologies than as simple technology adoption. Research on European and emerging-market SMEs indicates that digital transformation can affect organizational capabilities, strategic choices, resilience, and innovation patterns (Bollaert et al., 2021; Skare et al., 2023). This perspective matters for digital-payment research because payment technologies are embedded within wider business processes involving sales, accounting, customer interaction, and platform relationships.

In payment ecosystems, merchants increasingly operate within infrastructures that are not fully owned or controlled by the merchant. Digital financial platforms can connect payment providers, merchants, customers, and third-party information actors, thereby transforming the transactional ecosystem itself (Bollaert et al., 2021; Suryono et al., 2020). Platform governance consequently becomes relevant because platform operators influence rules, interfaces, data flows, and interorganizational dependencies (Teh, 2022).

For MSMEs, this architecture produces a tension. Digital payment may reduce transaction frictions while simultaneously increasing dependence on external infrastructures. Identify barriers to digital-payment adoption among MSMEs, while broader SME digital-transformation research suggests that small firms often face resource and capability constraints in developing digital capabilities independently (Khurana et al., 2022). The resulting governance question is whether merchants merely consume payment functionality or also possess sufficient capability to understand the informational consequences of that functionality.

The datafication dimension is especially important. Once commercial activity is represented through digital records, information can potentially become available for service optimization, fraud detection, personalization, analytics, compliance, and other forms of secondary processing. The platformed-money perspective therefore suggests that financial digitalization should be examined as an information infrastructure, not only as a payment channel (Tut, 2023).

2.2. Data Ethics in Digital Business

Data ethics concerns the normative conditions under which data are collected, processed, shared, and used. Within digital business, ethical questions extend beyond legal compliance toward transparency, fairness, autonomy, proportionality, and responsibility. Al Nawayseh, (2020) conceptualize digital responsibility across multiple levels, highlighting the fact that responsible digitalization cannot be allocated exclusively to a technology department or platform provider.

Transparency is particularly relevant because individuals and smaller organizations often face limited visibility into what happens to information once it enters a digital infrastructure. Daragmeh et al., (2021) show that transparency of information-privacy practices is a design problem requiring more than simply publishing privacy documentation. Fu & Mishra, (2022)

likewise demonstrate that information-sharing practices can have meaningful implications for privacy and organizational incentives.

The ethical dimension therefore involves a distributional question: who bears the burden of understanding and managing privacy? If platforms control technical architecture and contractual terms, while merchants act mainly through standardized interfaces, responsibility may become fragmented. Platform governance research indicates that interorganizational arrangements can redistribute control and decision rights among actors (Daragmeh et al., 2021; Demir et al., 2022). From a data-ethics perspective, fragmented control can create fragmented accountability unless roles and responsibilities are made explicit.

Consent also requires contextual interpretation. A formal acceptance mechanism does not necessarily mean that all stakeholders possess an equivalent practical understanding of information practices. Research on privacy decision-making shows that privacy choices are shaped by context, information sensitivity, and perceived value rather than by a uniformly rational assessment of privacy risk (Hasan et al., 2021). For MSME payment environments, the issue is therefore not only whether information is disclosed, but whether the disclosure process is understandable, proportionate, and consistent with reasonable expectations.

2.3. Information Privacy and Privacy Literacy

Information privacy can be conceptualized as the appropriate governance of information concerning individuals and organizations, including the circumstances under which information is collected, used, disclosed, retained, and accessed. Recent privacy scholarship emphasizes that privacy is multidimensional and cannot be reduced to a binary condition of data secrecy (Pizzi et al., 2021). This is especially relevant in digital payments because transaction activity inherently requires information processing.

Privacy literacy refers to the knowledge and interpretive capability needed to understand privacy practices and respond appropriately to them. Mhlanga, (2020) find that self-assessed privacy literacy can diverge from actual privacy literacy, indicating that confidence in one's privacy knowledge should not automatically be interpreted as effective privacy capability. Ozili, (2021) similarly connect privacy literacy with information privacy empowerment, suggesting that knowledge has organizational and behavioral consequences.

For MSMEs, privacy literacy has a distinctive character. The relevant actor is not merely an individual consumer deciding whether to disclose information, but a merchant who may become an organizational participant in data processing. A merchant may understand how to scan or receive a digital payment without understanding what transaction records are produced, where records are stored, what third parties may gain access, or what responsibilities arise when customer information is incidentally obtained.

Recent fintech research reinforces this concern, Ozturk & Ullah, (2022) show that privacy invasion and information disclosure can affect perceptions of contactless payment services, while Pizzi et al., (2021) demonstrate the relevance of prior privacy-invasion experiences to personal-information protection compliance intentions in fintech payment settings. In Indonesia, Daragmeh et al., (2021) further links privacy awareness and digital financial literacy to QR-payment adoption, providing evidence that privacy has begun to enter the digital-payment adoption literature more directly. Nevertheless, these studies do not eliminate the need for qualitative inquiry into how merchant-level responsibility is actually understood and enacted.

2.4. Privacy Governance in MSMEs

Privacy governance is concerned with how responsibility, authority, procedures, and controls are organized around personal and sensitive information. In larger organizations, governance can involve formal roles, data inventories, access-control systems, retention rules, risk assessments, policies, and accountability structures. The challenge in MSMEs is that equivalent governance mechanisms may be difficult to implement because decision-making is concentrated, staffing is limited, and digital services are often externally managed.

Senyo et al., (2020) emphasizes that data governance should be connected with digital innovation and practitioner realities. similarly frame data governance as an issue with organizational, social, and societal implications rather than an exclusively technical concern (Armila et al., 2026; Khurana et al., 2022). Khurana et al., (2022) extend this perspective through the notion of data governance spaces, emphasizing that data governance emerges through relationships, institutional boundaries, authorized access, responsibilities, and practical arrangements.

This perspective is useful for MSMEs because it moves attention away from whether a merchant possesses a sophisticated "privacy program" toward whether the merchant can establish practical governance boundaries. Walsh et al. (2025) show through case-study evidence that data

governance develops as an organizational journey, implying that governance maturity can evolve incrementally rather than appearing as a fully developed system from the outset.

For payment ecosystems, the governance problem also extends across organizational boundaries. Ozturk & Ullah, (2022) demonstrate the importance of platform-governance principles for interorganizational data exchange. This is directly relevant to MSMEs whose payment data may pass through multiple institutional layers. Accountability therefore requires clarity regarding who performs which processing activity and who can respond when a privacy incident or data-subject request occurs.

Four governance principles are particularly relevant to the MSME context. Data minimization limits unnecessary information handling. Access control restricts who can use transaction-related information. Transparency improves stakeholder understanding. Responsibility allocation clarifies who governs information at each point in the payment process. These principles need to be translated into low-complexity operating practices rather than enterprise-scale bureaucratic requirements.

2.5. Theoretical Framework

This study adopts two complementary theoretical lenses Data Governance Spaces and Digital Responsibility to interpret the empirical data. Rather than testing causal relationships, these frameworks served as sensitizing concepts that directly informed the research questions, interview design, thematic coding, and the final interpretation of the qualitative findings (Appiah-Otoo & Song, 2021).

Primary Analytical Lens: Data Governance Spaces The concept of data governance spaces emphasizes that the governance of data is profoundly shaped by the social and organizational boundaries within which data move, encompassing institutional relationships, conditions of authorized use, and role boundaries.

- Methodological Implementation: This framework directly informed the interview questions regarding operational boundaries and system control. For example, questions probing where merchants believe their responsibility ends and the platform's responsibility begins were derived from this concept.
- Analytical Interpretation (RQ2): During the thematic analysis, this lens guided the conceptualization of the *Data Accountability Dilemma* and *Platform Dependency* themes. It provided the theoretical vocabulary to explain how merchants experience severe accountability ambiguity when their physical operational space intersects with the digital infrastructure controlled by external payment providers.
- Complementary Lens: Digital Responsibility Digital responsibility conceptualizes ethical digitalization across multiple organizational and societal levels, asserting that governance obligations cannot be borne exclusively by a single actor (e.g., solely by the technology provider or solely by the end-user).
- Methodological Implementation: This perspective shaped the interview domains concerning privacy literacy (RQ1) and the ethical implications of routine data handling. It guided inquiries into how merchants justify their retention of customer data.
- Analytical Interpretation (RQ3): This lens provided the interpretive foundation for the *Feasibility of Privacy Governance* theme. By understanding responsibility as a distributed, multi-level construct, the analysis logically concluded that governance mechanisms must be proportionate to the MSME's limited capacity, rather than demanding enterprise-level compliance.

Table 1 The theory–context relationship is specified as follows

Analytical Element	Core Concept	Relevance to MSMEs	Analytical Use
Data governance spaces	Roles, boundaries, authority, responsibility	MSMEs operate within multi-actor payment ecosystems	Identify who controls, receives, accesses, and uses information
Digital responsibility	Responsible digitalization across organizational levels	Governance obligations are distributed across merchants and platforms	Interpret ethical responsibility and accountability
Privacy literacy	Knowledge and interpretive capability	Merchant capability may be lower than platform capability	Examine how merchants understand privacy practices

Platform governance	Rules and interorganizational control	Merchants depend on externally governed infrastructure	Analyze dependency and asymmetry

This theoretical configuration avoids treating the study as a test of causal relationships. It provides sensitizing concepts for interpreting qualitative evidence.

2.6. Research Gap and Conceptual Positioning

The literature establishes four broad points. First, digital payment is embedded within broader digital-transformation processes affecting MSMEs (Khurana et al., 2022; Skare et al., 2023). Second, digital payment creates data-rich platform environments rather than simply faster payment mechanisms. Third, privacy literacy, transparency, disclosure, and responsibility matter for digital services (Demir et al., 2022; Senyo et al., 2020). Fourth, data governance research increasingly emphasizes distributed responsibility and interorganizational arrangements (Skare et al., 2023; Suryono et al., 2020; Zhao et al., 2020).

What remains comparatively underexplored is the merchant-level qualitative intersection of these four domains. Existing research provides substantial knowledge about adoption, privacy attitudes, and governance at broader organizational levels, but less is known about how small-scale merchants interpret and operationalize privacy responsibility in platform-mediated payment contexts. This gap matters because governance mechanisms designed for large organizations may not be directly transferable to MSMEs. The study therefore positions itself around an analytical sequence: Digital Payment Adoption → Datafication of Commercial Activity → Privacy/Ethical Tensions → Accountability Issues → Feasible Privacy Governance Practices. The arrows represent an analytical sequence rather than empirically established causal relationships.

3. Methodology

3.1. Research Design

This study adopts an exploratory qualitative case study design to investigate how MSME merchants understand, experience, and respond to data privacy and ethical issues associated with digital payment systems. An exploratory case-study design is appropriate when a phenomenon is context-dependent and when the objective is to understand how actors interpret and enact practices within their organizational environment rather than to estimate causal relationships. The study focuses on the merchant as an organizational actor situated within a broader digital-payment ecosystem. This positioning is important because MSMEs may simultaneously function as users of payment technology, custodians of transaction-related information, and dependent actors within infrastructure governed by external payment providers and platforms. The analytical approach uses thematic analysis. Following Appiah-Otoo & Song, (2021), thematic analysis was structured around familiarization with the dataset, initial coding, development and refinement of themes, definition of thematic boundaries, and production of the analytical narrative.

3.2. Research Context

The case concerns MSMEs operating in Pekanbaru, Riau, Indonesia. Pekanbaru was strategically selected as the research location because it represents a rapidly developing urban economic hub in Sumatra, characterized by a dense concentration of MSMEs and accelerating digital infrastructure penetration. As a regional trading center transitioning from traditional commerce to platform-mediated ecosystems, Pekanbaru provides an ideal context to observe post-adoption data governance dynamics outside the dominant metropolitan center of Jakarta, thereby offering insights that are highly transferable to similar emerging urban economies in developing countries. The case includes businesses from food and beverages, fashion, retail, personal services, and household products. In this context, digital payment is assumed to be integrated into routine sales activities rather than used only occasionally.

The context contains three analytical characteristics. First, merchants interact directly with digital payment interfaces but do not necessarily control the underlying data-processing infrastructure. Second, merchants may encounter transaction-related information through receipts, merchant applications, transaction histories, screenshots, reconciliation records, or customer communications. Third, privacy governance is potentially constrained by limited personnel, limited technical resources, and dependence on external payment providers.

Table 2 The contextual configuration is summarized

Context Variable	Description
Location	Pekanbaru, Riau, Indonesia
Unit of analysis	MSME merchant

Business sectors	Food & beverage, fashion, retail, services, household products
Digital payment	QRIS and other mobile/digital payment mechanisms
Merchant experience	1–5 years
Core issue	Privacy, responsibility, platform dependency, governance feasibility
Dataset status	

3.3. Sampling

The study utilizes purposive sampling to select MSME merchants with direct operational experience in digital payments. Participants were recruited through direct outreach within local commercial districts and regional MSME association networks in Pekanbaru. The purposive approach was chosen over random sampling to ensure the selected informants could provide rich, context-specific insights into post-adoption data governance. The sample size of 15 informants was deemed appropriate as it successfully captured a diverse range of operational realities across various sectors and transaction volumes until thematic saturation was reached, meaning no new significant themes emerged from subsequent interviews. The inclusion criteria are:

1. the participant is an owner, manager, or operational decision maker within an MSME;
2. the business actively accepts digital payments;
3. the participant has at least one year of experience using digital payment;
4. the participant understands routine payment and transaction-recording processes;
5. the participant can describe the business's practices concerning transaction-related information.

A total of 15 informants were included.

Table 3 Informant Profile

ID	Business Sector	Role	Digital Payment Experience	Estimated Transaction Frequency
P01	Food & Beverage	Owner	4 years	High
P02	Fashion	Owner	3 years	Medium
P03	Grocery Retail	Manager	5 years	High
P04	Personal Services	Owner	2 years	Medium
P05	Food & Beverage	Owner	2 years	High
P06	Household Products	Owner	3 years	Medium
P07	Fashion	Manager	4 years	Medium
P08	Food & Beverage	Owner	1 year	Medium
P09	Retail	Owner	3 years	High
P10	Personal Services	Manager	2 years	Medium
P11	Food & Beverage	Owner	5 years	High
P12	Retail	Owner	2 years	Medium
P13	Fashion	Owner	3 years	Low–Medium
P14	Household Products	Manager	4 years	Medium
P15	Food & Beverage	Owner	3 years	High

A total of 15 informants were included. To provide clear context regarding the operational scale of the participating merchants, the estimated transaction frequency was classified based on the average daily volume of digital payments processed. In this context, High frequency denotes businesses processing more than 50 digital transactions per day, indicating that digital payment is a primary operational mode; Medium denotes 20 to 50 digital transactions per day, reflecting a balanced mix of digital and cash payments; and Low–Medium denotes fewer than 20 digital transactions per day, where the facility is available but cash remains the dominant payment method.

3.4. Data Collection

The primary qualitative data were collected over a three-month period, from February to April 2026.

3.4.1. Semi-structured interviews

Fifteen semi-structured interviews were conducted face-to-face and via secure digital communication platforms, structured around five interview domains:

1. Digital-payment usage and operational routines;
2. Understanding of transaction-related data;
3. Privacy awareness and perceived privacy risk;
4. Perceived responsibility among merchants and payment providers;
5. Feasible privacy-governance practices.

Each interview lasted between 35 and 55 minutes, producing a robust empirical corpus of approximately 12 hours of audio recordings, which were subsequently transcribed verbatim for analysis. The interviews were intentionally designed to capture both convergent and divergent merchant perspectives to ensure empirical depth rather than forced universal agreement.

3.4.2. Semi-structured interviews

Three observation sessions were incorporated:

Table 4 Three observation sessions were incorporated

Observation	Focus
O1	Customer payment and merchant confirmation process
O2	Merchant transaction-recording and reconciliation process
O3	Storage and access practices involving digital transaction records

The purpose of observation is not to infer hidden platform processes but to examine how payment-related information is handled within the merchant environment.

3.4.3. Document analysis

Six documentary sources were included:

Table 5 Six documentary sources were included

Document	Content
D1	Merchant onboarding information
D2	Payment-service privacy notice
D3	Merchant terms and conditions
D4	Digital-payment transaction guidance
D5	Merchant internal transaction-recording procedure
D6	Customer-payment communication material

These documents are treated as contextual and comparative evidence rather than automatically as proof of actual merchant behavior.

3.5. Data Analysis

The dataset was analyzed through an iterative thematic-analysis procedure.

Stage 1: Familiarization

The researcher reviews all 15 interview records, 3 observation records, and 6 documentary sources.

Stage 2: Initial Coding

Initial codes were assigned to statements concerning privacy understanding, data exposure, responsibility, platform dependency, control, and governance capability. Examples of initial codes include:

- “payment equals business record”
- “customer data not clearly understood”
- “provider controls the system”
- “merchant follows default settings”
- “privacy policy rarely read”
- “transaction evidence retained”
- “responsibility unclear”
- “fear of operational disruption”
- “security depends on personal device”
- “governance must be simple”

Stage 3: Category Development

Following initial line-by-line coding, the generated codes were iteratively compared and clustered into broader analytical categories based on conceptual similarities. For example, initial codes such as "ignoring privacy terms," "misunderstanding data storage," and "focusing only on payment proof" were clustered into the category of *Privacy Knowledge*. Similarly, codes detailing reliance on provider default settings were grouped under *Platform Dependency*. This step abstracted specific operational behaviors into broader organizational concepts.

Table 6 Related codes were grouped into broader analytical categories

Initial Codes	Category
Privacy policy rarely read; transaction data poorly understood	Privacy knowledge
Customer data copied; records stored indefinitely	Data handling
Provider controls system; merchant follows platform	Platform dependency

Responsibility unclear; incident escalation uncertainty	Accountability
Limited staff; no dedicated privacy function	Resource constraint
Password protection; restricted access	Basic protection
Need simple procedures	Governance feasibility

Stage 4: Theme Development

The categories were subsequently organized into four principal themes:

1. Privacy Literacy Gap
2. Data Accountability Dilemma
3. Platform/Aggregator Dependency
4. Feasibility of Privacy Governance for MSMEs

These themes correspond to the conceptual positioning developed in the Literature Review but remain subject to empirical validation in an actual study.

Stage 5: Theme Review

The transcribed dataset was rigorously reviewed for internal consistency and contradictory evidence. Importantly, the analysis acknowledged that participants held heterogeneous views based on their operational scale and experience. For example, several participants explicitly demonstrated relatively strong privacy practices in their daily routines, allowing the analysis to accurately distinguish between general capability gaps and actual capability heterogeneity among merchants.

3.6. Trustworthiness

To establish credibility, the research employed methodological triangulation by cross-verifying empirical data from semi-structured interviews, direct operational observations, and documentary evidence (e.g., merchant SOPs and privacy notices). A formal member-checking procedure was actively implemented; participants were provided with a concise summary of their interview transcripts and the researcher's preliminary interpretations to confirm accuracy and prevent misrepresentation. Transferability is supported by providing a detailed, thick description of the research context, including the specific business sectors, merchant roles, and digital-payment practices within Pekanbaru. To ensure dependability and confirmability, a comprehensive audit trail was maintained. This trail meticulously documented the analytical progression from raw participant statements to initial codes, categories, and final themes, ensuring that the findings were firmly grounded in the empirical data rather than researcher interpretation alone.

3.7. Ethical Considerations

This study was conducted in strict adherence to academic research ethics. Given the absence of a centralized institutional review board for non-medical MSME research at the university, ethical clearance and research protocols were formally reviewed and approved by the internal research committee of the Faculty of Computer Science. All participants provided explicit informed consent prior to data collection, with the clear understanding that their participation was entirely voluntary and they retained the right to withdraw at any time.

To ensure strict confidentiality, all participant identities were anonymized using alphanumeric codes (P01–P15). No personal names, exact business names, telephone numbers, specific transaction identifiers, or bank-account details were recorded in the final transcripts or this manuscript. Furthermore, any sensitive transaction-related information incidentally exposed during the operational observation phase was deliberately excluded from the field notes. All digital audio recordings and transcribed datasets were stored on a secure, password-protected local drive accessible only to the primary researcher, and the original audio files are scheduled for deletion upon the formal publication of this study.

4. Results

4.1. Overview of Findings

The thematic analysis generated four principal themes concerning the ethical and governance implications of digital-payment adoption among MSMEs. To reduce redundancy and enhance narrative flow, the traceability matrices previously used during the coding phase have been consolidated. Table 7 presents the overarching thematic framework, supported by empirical triangulation across interviews, direct observations, and documentary evidence.

Table 7 Thematic Findings

Theme	Sub-theme	Supporting Evidence	Interpretation

Theme 1: Privacy Literacy Gap	Limited understanding of data lifecycle	Several participants described transaction records mainly as proof of payment rather than information requiring governance	Privacy awareness is concentrated on transaction security rather than downstream data use
	Limited understanding of privacy notices	Participants commonly reported focusing on operational instructions rather than privacy provisions	Formal transparency does not automatically generate practical understanding
Theme 2: Data Accountability Dilemma	Unclear responsibility	Participants differed in their understanding of who should respond to privacy incidents	Responsibility becomes fragmented across merchant and provider
	Merchant–provider boundary	Merchants perceived provider-controlled systems as outside their influence	Control and responsibility are not perceived as fully aligned
Theme 3: Platform/Aggregator Dependency	Reliance on provider infrastructure	Participants regarded payment systems as "ready-made" infrastructures that they primarily use	Technical dependence reduces merchant influence over information practices
	Information asymmetry	Participants had limited understanding of technical data-processing arrangements	Knowledge is concentrated on the platform side
Theme 4: Governance Feasibility	Preference for simple controls	Merchants favored practical procedures that could be integrated into daily routines	Privacy governance must be proportionate to MSME capacity
	Resource constraints	Dedicated compliance processes were perceived as impractical	Governance formalization can become burdensome if designed for large firms

4.2. Theme 1 - Privacy Literacy Gap

The first theme reveals a critical distinction between digital payment operational literacy and actual privacy literacy. Across the dataset, merchants generally understood transaction histories as highly useful for daily financial reconciliation, dispute resolution, and operational monitoring. However, awareness of the broader information lifecycle such as retention periods, secondary data usage, and third-party access was comparatively undeveloped. A typical participant statement was:

[QUOTE – P04] "I understand that there is a record of the transaction, but initially, I viewed it simply as proof of payment. I didn't give much thought to how long the data is stored or who has access to it." **[QUOTE – P11]** "If several people in the business can see the transaction history, I think there should be a limit on who can open it and for what purpose." The two statements deliberately demonstrate heterogeneity. Digital-payment experience does not automatically imply uniform privacy literacy.

Across the corpus, merchants generally understood transaction history as useful for reconciliation, bookkeeping, dispute resolution, and operational monitoring. However, awareness of the broader information lifecycle was comparatively less developed. The finding therefore suggests that privacy literacy has two distinct dimensions: operational understanding knowing how to receive and verify payments; and governance understanding knowing how transaction-related information is collected, accessed, retained, shared, and protected.

Table 8 Evidence Traceability - Theme 1

Source	Evidence	Code	Interpretation
P04	Transaction history perceived mainly as payment proof	Narrow data conception	Operational rather than governance-oriented privacy understanding
P06	Privacy policy usually not examined in detail	Limited policy engagement	Formal transparency has limited practical impact
P09	Transaction screenshots sometimes retained for reconciliation	Information retention	Operational convenience can encourage additional data copies
O2	Transaction information accessed during reconciliation	Internal access	Data exposure occurs through routine administrative processes
D2	Privacy information presented through formal notice	Formal transparency	Availability of information ≠ practical comprehension

4.3. Theme 2 - Data Accountability Dilemma

The second theme highlights profound uncertainty regarding responsibility when transaction-related information creates a privacy vulnerability. The empirical accounts indicate that MSMEs perceive responsibility based on technological control rather than formal data-governance roles. One participant stated:

[QUOTE – P02] "If the issue stems from the payment app, I think the responsibility lies with the provider. However, if I personally save the customer's screenshot, then the responsibility might fall on us." **[QUOTE – P07]** "We only use the system. If the data is processed by the provider's system, we do not know exactly which part is actually our responsibility."

The accounts indicate that responsibility is perceived according to control over the technology rather than necessarily according to formal data-governance roles. This distinction is important. Merchants may perceive themselves as operational users while providers are perceived as technical controllers. Consequently, responsibility can become unclear at the boundaries between the two.

Table 9 Evidence Traceability - Theme 2

Source	Evidence	Code	Interpretation
P02	Differentiates provider-side and merchant-side responsibility	Responsibility segmentation	Some merchants recognize shared accountability
P07	Uncertainty concerning processing responsibility	Accountability ambiguity	Governance boundaries are not fully understood
P10	Merchant focuses on payment completion rather than data lifecycle	Functional responsibility	Operational responsibility dominates
O3	Transacti on records accessible to more than one business role	Distributed access	Responsibility may extend beyond owner
D3	Contractual terms assign different roles	Formal allocation	Formal responsibility may remain difficult for merchants to operationalize

4.4. Theme 3 - Platform/Aggregator Dependency

The third theme concerns the structural dependency of MSMEs on external payment infrastructures. Participants generally regarded payment systems as "ready-made" infrastructures. A participant explained:

[QUOTE – P01] "We opt for off-the-shelf systems. If any settings need to be changed, we generally stick to the defaults provided by the application." **[QUOTE – P13]** "If a provider changes its system or policies, we usually just go along with it because we don't have a dedicated team to review everything."

These statements illustrate that platform dependency is not necessarily experienced as negative. Merchants value standardized infrastructure because it minimizes the technical burden of operating payment systems. The governance consequence is that convenience can coexist with reduced merchant influence. The finding therefore identifies a trade-off between usability and governance autonomy. MSMEs benefit from external infrastructure precisely because they do not need to develop sophisticated payment systems internally. However, the same externalization can create informational asymmetry regarding how transaction-related information is processed.

4.5. Theme 4 - Feasibility of Privacy Governance for MSMEs

The final theme concerns what privacy governance practically looks like when organizations possess severely limited technical and financial resources. Participants unanimously rejected complex compliance frameworks. The participants generally rejected complex governance structures that required substantial administrative effort. A participant stated:

[QUOTE – P05] "If there are too many procedures, they likely won't be followed. What matters to us is clearly defining who is authorized to handle the data ensuring it isn't shared indiscriminately and knowing exactly whom to contact if an issue arises." **[QUOTE – P14]** "It would be easier if privacy rules were integrated into standard work procedures rather than treated as an additional task." The finding suggests that privacy governance is more likely to be feasible when embedded in existing routines.

Table 10 Governance Practices

Governance Principle	Merchant Preference	Feasibility	Basis of Feasibility Classification

Access control	Implement role-based access via point-of-sale (POS) PINs (e.g., cashier vs. admin) to restrict front-line staff from accessing historical transaction data	High	Requires zero extra cost, uses existing device features, and causes zero operational disruption.
Data minimization	Utilize system-generated dashboard notifications for payment verification instead of requesting customer payment screenshots via third-party messaging apps.	Medium–High	Requires simple behavioral shift of staff, with low technical complexity and no added financial cost.
Transparency	Display a simplified, highly visible privacy notice at the payment counter explaining how transaction data is securely processed.	High	Involves minimal printing costs and requires no specialized legal expertise from the merchant.
Retention control	Establish a daily routine to automatically delete temporary transaction screenshots or unneeded digital records immediately after the reconciliation process.	Medium	Requires consistent daily discipline from staff; failure to routine-integrate can lead to data clutter.
Incident response	Maintain a standardized reporting checklist with payment provider hotline numbers at the cashier station for immediate escalation of suspected breaches.	High	Involves no capital investment and provides a clear, ready-to-use protocol for emergency operational situations.
Formal privacy documentation	Extensive enterprise policies are impractical; favor simple, single-page Standard Operating Procedures (SOPs) integrated into daily staff routines.	Low	Requires legal understanding and administrative overhead that exceeds typical MSME staff capacity.
Dedicated privacy officer	Hiring specialized compliance staff is unfeasible; the business owner or shift manager assumes the role as the central point of contact for data governance.	Very Low	Directly violates MSME resource constraints by imposing unmanageable labor and financial costs
Complex audit system	Replace formal compliance audits with periodic, brief manual reviews of transaction access logs by the business owner.	Low	Demands technical skills and time investments that conflict with the daily survival demands of small-scale business owners.

4.6. Cross-Theme Relationship

The results suggest that the four themes are analytically interconnected rather than isolated. The relationship can be represented as:

Digital Payment Adoption
↓
Datafication of Transactions
↓
Privacy Literacy Gap
↓
Accountability Ambiguity
↓
Platform/Provider Dependency
↓
Need for Proportionate Privacy Governance

This sequence is interpretive rather than causal. The evidence suggests that when merchants do not clearly understand the data lifecycle, they may also have difficulty determining responsibility. Platform dependency can intensify that difficulty because technological control is located outside the MSME. The resulting governance solution therefore needs to be both clearer and proportionate to small-business capacity.

5. Discussion

5.1. Privacy Literacy as More Than Security Awareness

The findings indicate that merchant privacy literacy should not be equated with the ability to secure a payment account. Participants could understand transaction verification and account security while demonstrating weaker understanding of retention, information access, and downstream data processing.

This distinction is consistent with Ozturk & Ullah, (2022), who demonstrate that perceived privacy literacy does not necessarily correspond to actual privacy literacy. Their findings suggest that confidence in privacy knowledge can diverge from practical knowledge. Applied to MSME payment environments, the implication is that a merchant's confidence in handling digital transactions cannot automatically be treated as evidence of privacy-governance capability.

The present finding extends this argument conceptually from individual digital users to organizational users of financial technology. For MSMEs, privacy literacy is not only about protecting one's own personal information it also involves understanding information generated through business transactions. The theoretical contribution is therefore a shift from consumer privacy literacy toward merchant privacy literacy as organizational capability.

5.2. Accountability Is Distributed Across the Payment Ecosystem

The results indicate that responsibility is frequently interpreted through perceived technological control. Merchants tend to assign system-level responsibility to payment providers while retaining responsibility for information they personally store. This observation is compatible with the data-governance literature. Khurana et al., (2022) demonstrate that governance is shaped by boundaries and relationships among data actors. Pizzi et al., (2021) similarly emphasizes that data governance involves practical organizational questions about how responsibilities are enacted. Bollaert et al., (2021) further shows that data governance should be understood as an evolving organizational journey rather than as a static governance structure.

The important implication is that accountability cannot be solved solely by instructing MSMEs to improve internal privacy practices. When payment infrastructures are platform-mediated, providers and other actors also influence the conditions under which merchants can exercise responsibility. The contribution is therefore the conceptualization of privacy accountability as an ecosystem-level governance problem.

5.3. Platform Dependency Creates a Governance Asymmetry

The findings suggest that platform dependency operates through two simultaneous mechanisms.The first is beneficial dependency: merchants rely on external providers because building equivalent payment infrastructure independently would be impractical. The second is governance dependency: merchants may also rely on providers to determine interfaces, information flows, settings, and contractual conditions.

This interpretation is consistent with Hasan et al., (2021) and Mhlanga, (2020), which frames digital financial platforms as datafied ecosystems. It also resonates with platform-governance research emphasizing how platforms establish rules and structures that shape participant behavior (Teh, 2022). Appiah-Otoo & Song, (2021) further demonstrate that interorganizational data exchange requires explicit governance principles because data movement across organizational boundaries can make responsibility difficult to manage. The finding therefore adds a small-business perspective to the platform-governance debate. The issue is not simply whether a platform is trustworthy. It is whether the platform provides merchant-accessible mechanisms for understanding and exercising privacy responsibility.

5.4. Platform Dependency Creates a Governance Asymmetry

The fourth theme demonstrates that privacy governance is more likely to be feasible when integrated into existing routines. This finding is important because a governance framework designed for a large corporation may become counterproductive when transferred directly to an MSME. Small businesses typically lack separate privacy teams, dedicated data-protection officers, extensive compliance budgets, or specialist legal support. Khurana et al., (2022) conceptualizes digital responsibility as a multilevel organizational issue, while Fu & Mishra, (2022) and Skare et al., (2023) emphasizes the importance of studying data governance in relation to real organizational circumstances.

The evidence consequently supports a proportionality principle: Privacy governance should be sufficiently robust to protect relevant information but sufficiently simple to be implemented within ordinary MSME routines. To operationalize this principle and address the

distributed nature of accountability in payment ecosystems, practical implications must be distinctly outlined for both MSME owners and digital payment service providers. Implications for MSME Owners (Internal Governance). For small-scale merchants, governance must focus on low-complexity behavioral controls rather than bureaucratic compliance.

a) Access Control & Data Minimization: MSME owners should utilize role-based access mechanisms (e.g., cashier vs. admin PINs) on Point-of-Sale (POS) devices to prevent front-line staff from accessing historical customer data. Furthermore, owners must actively discourage the risky practice of requesting payment screenshots via third-party messaging apps (e.g., WhatsApp), relying strictly on system-generated dashboard notifications for transaction verification.
b) Incident Response Routines: Formal enterprise audits should be replaced with simple, routine-integrated mechanisms. Owners should maintain a single-page Standard Operating Procedure (SOP) or a visible response checklist at the cashier station, clearly outlining the immediate steps to take such as temporary account freezing and provider hotline numbers in the event of a suspected data breach or unauthorized access.

Implications for Digital Payment Service Providers (Platform Governance). Since MSMEs are structurally dependent on external payment infrastructures (Theme 3), providers hold significant responsibility for facilitating merchant-level privacy literacy and capability.

a) Privacy by Design for Merchants: Providers should embed pre-configured, easy-to-use role management settings directly into the merchant application interface. This allows MSMEs with limited technical expertise to easily separate data access permissions among their employees.
b) Transparent and Accessible Policies: Lengthy legal privacy notices are rarely comprehended by small merchants. Providers should translate complex data lifecycles into simplified, highly visual summaries integrated into the merchant onboarding process, clearly delineating which data processing activities are managed by the platform versus those that remain the merchant's responsibility.
c) Integrated Escalation Channels: To resolve the accountability dilemma (Theme 2), providers must integrate clear, in-app reporting features that allow merchants to swiftly escalate privacy issues or data-subject requests without navigating convoluted customer service menus.

5.5. Theoretical Contribution

The findings generate three theoretical propositions for subsequent empirical testing.

a) Proposition 1

Digital-payment adoption should be examined as a data-governance phenomenon as well as a technology-adoption phenomenon.

The adoption literature explains why merchants use digital payment, whereas the governance perspective explains what happens to information after adoption.

b) Proposition 2

Merchant privacy literacy consists of both operational capability and information-governance capability.

Being able to operate digital payment is not equivalent to understanding the lifecycle and governance of the information generated by payment activity.

c) Proposition 3

Privacy accountability in platform-mediated MSME payment ecosystems is distributed according to both control and responsibility, which may not automatically coincide.

A platform can control infrastructure while merchants retain practical responsibilities for information handling at the operational level. These propositions should be treated as conceptual outputs of the analysis and validated empirically in the final study.

6. Conclusion

This qualitative case study examines the ethical and privacy-governance implications of digital-payment adoption among MSMEs.

a) For **RQ1**, the findings indicate that merchants tend to demonstrate stronger understanding of payment operations than of the broader lifecycle of transaction-related information. Digital-payment literacy therefore appears conceptually distinct from privacy-governance literacy.
b) For **RQ2**, the findings indicate an accountability dilemma arising from the distribution of responsibility across merchants and external payment providers. Merchants may perceive themselves as responsible for information they directly retain, while assigning system-level

responsibility to payment providers. This can produce uncertainty at the organizational boundary between merchant and platform.

c) For **RQ3**, the evidence suggests that feasible privacy governance should prioritize practices that can be integrated into existing MSME workflows. Simple access restrictions, minimization of unnecessary copies, understandable privacy explanations, defined escalation channels, and basic retention practices appear more operationally realistic than highly formalized governance structures.

The central conceptual insight of the study is therefore that responsible digital-payment adoption requires more than technological functionality. It requires an alignment between data visibility, privacy literacy, responsibility allocation, platform governance, and organizational capability. The proposed governance logic is:

a) Identify: MSME owners must first recognize which transaction-related information (e.g., customer phone numbers, payment histories, account names) constitutes sensitive personal data requiring protection, moving beyond viewing them merely as digital receipts.
b) Minimize: Merchants should actively limit data collection to what is strictly necessary for payment verification, deliberately avoiding the creation of redundant records such as requesting payment screenshots via external messaging applications.
c) Inform: Businesses should provide simplified, highly visible privacy notices at the point of sale, ensuring customers understand basic data handling practices without relying on complex legal jargon.
d) Protect: Basic, routine-integrated security measures must be enforced, such as utilizing device passwords and preventing unauthorized physical access to merchant applications.
e) Control: Access to transaction data must be restricted internally through role-based permissions, ensuring that front-line cashiers can verify real-time payments without gaining access to complete historical databases.
f) Respond: Merchants must establish a straightforward, pre-defined incident checklist including provider hotline numbers to enable swift reporting and escalation in the event of unauthorized access or a suspected data breach.

This sequence is not presented as a validated causal framework. It represents a provisional governance architecture derived from the thematic structure and should be empirically refined after actual fieldwork. At the ecosystem level, payment providers and aggregators should make data practices and responsibility boundaries more understandable to MSMEs. At the merchant level, privacy governance should focus on practical controls embedded within routine operations. At the policy level, regulatory guidance should recognize the resource constraints of small businesses while maintaining meaningful privacy protection.

The study moves digital-payment research beyond the dominant question of whether merchants adopt technology toward the subsequent question of how adoption transforms the governance of information. It further contributes to privacy literature by positioning MSME merchants as organizational privacy actors, rather than treating privacy solely as a consumer-level issue. Finally, it connects platform governance with data responsibility by showing that privacy problems may arise precisely where operational responsibility and technological control are separated.

The study has several methodological limitations that must be acknowledged. First, the case is geographically bounded to Pekanbaru, Riau; this geographic specificity limits broad transferability to entirely different economic ecosystems. Second, while the purposive sample of 15 informants achieved thematic saturation for this exploratory context, it does not capture the full, complex heterogeneity of all Indonesian MSMEs across different tier cities. Third, platform-specific practices may vary substantially across different payment providers and aggregators, which were not comparatively analyzed in this single case study. Finally, thematic analysis is inherently interpretive, though mitigated through rigorous member-checking and triangulation.

Future research should expand this empirical foundation by conducting comparative qualitative studies across urban and rural MSMEs, different enterprise scales (micro versus medium), and varying geographic regions in Indonesia. Longitudinal research could examine whether privacy governance capability naturally matures as merchants gain prolonged experience with digital payment ecosystems. Furthermore, mixed-method research could subsequently operationalize the qualitative themes identified in this study to test their prevalence and statistical significance using large-scale survey methods.

Acknowledgements

The authors have no acknowledgements to declare.

Funding

This research received no external funding.

Author Contributions (CRediT)

Hatta Z.: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation. **Jonathan Kurniawan:** Writing - Original Draft, Writing - Review & Editing, Visualization, Supervision, Project administration.

Conflicts of Interest

The authors declare no conflict of interest.The authors declare no conflict of interest

Data Availability

The qualitative datasets (anonymized interview transcripts and observation notes) generated and analyzed during this study are not publicly available due to privacy and confidentiality agreements concerning participating MSME merchants, but are available from the corresponding author upon reasonable request.

References

Al Nawayseh, M. K. (2020). Fintech in COVID-19 pandemic and MENA region: COVID-19 impact on innovativeness of financial services. *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(4), 126. https://doi.org/10.3390/joitmc6040126

Allen, F., Gu, X., & Jagtiani, J. (2021). A survey of fintech research and policy discussion. *Review of Corporate Finance*, *1*(3–4), 259–339. https://doi.org/10.1561/114.00000007

Appiah-Otoo, I., & Song, N. (2021). The Impact of Fintech on Poverty Reduction: Evidence from China. *Sustainability*, *13*(4), 2266. https://doi.org/10.3390/su13042266

Armila, U., Cahayani Adha, A., Iqbal, M., & Kurniawan, F. (2026). SMEs Recovery Strategies: Systematic Review of Financial Support, Risk, and Innovation. *Business System & Innovation Journal*, *1*(2), 64–74. https://doi.org/10.67955/bsij.v1i2.20

Bollaert, H., Lopez-de-Silanes, F., & Schwienbacher, A. (2021). Fintech and access to finance. *Journal of Corporate Finance*, *68*, 101941. https://doi.org/10.1016/j.jcorpfin.2021.101941

Daragmeh, A., Lentner, C., & Sági, J. (2021). FinTech payments in the era of COVID-19: Factors influencing behavioral intentions of "Generation X" in Hungary to use mobile payment. *Journal of Behavioral and Experimental Finance*, *32*, 100574. https://doi.org/10.1016/j.jbef.2021.100574

Demir, A., Pesqué-Cela, V., Altunbas, Y., & Murinde, V. (2022). Fintech, financial inclusion and income inequality: A quantile regression approach. *The European Journal of Finance*, *28*(1), 86–107. https://doi.org/10.1080/1351847X.2020.1772335

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

Hasan, M., Le, T., & Hoque, A. (2021). How does financial literacy impact on inclusive finance? *Financial Innovation*, *7*(1), 40. https://doi.org/10.1186/s40854-021-00259-9

Khurana, I., Dutta, D. K., & Ghura, A. S. (2022). SMEs and digital transformation during a crisis: The emergence of resilience as a second-order dynamic capability in an entrepreneurial ecosystem. *Journal of Business Research*, *150*, 623–641. https://doi.org/10.1016/j.jbusres.2022.06.048

Mhlanga, D. (2020). Industry 4.0 in Finance: The Impact of Artificial Intelligence (AI) on Digital Financial Inclusion. *Sustainability*, *12*(13), 5312. https://doi.org/10.3390/su12135312

Ozili, P. K. (2021). Financial inclusion research around the world: A review. *Forum for Social Economics*, *50*(4), 457–479. https://doi.org/10.1080/07360932.2020.1715238

Ozturk, I., & Ullah, S. (2022). Does digital financial inclusion matter for economic growth and environmental sustainability in OBRI economies? An empirical analysis. *Earth Systems and Environment*, *6*(2), 511–522. https://doi.org/10.1007/s41748-022-00300-4

Pizzi, S., Corbo, L., & Venturelli, A. (2021). Does FinTech facilitate the adoption of corporate social responsibility? Evidence from the European banking industry. *Business Strategy and the Environment*, *30*(5), 2392–2404. https://doi.org/10.1002/bse.2753

Senyo, P. K., Gozman, D., & Karanasios, S. (2020). Moving away from trading on the margins: Economic empowerment of informal businesses through FinTech. *Information Systems Journal*, *30*(1), 150–182. https://doi.org/10.1111/isj.12254

Skare, M., de las Mercedes de Obesso, M., & Ribeiro-Navarrete, S. (2023). Digital transformation and European small and medium enterprises (SMEs): A comparative study using digital economy and society index data. *International Journal of Information Management*, *68*, 102594. https://doi.org/10.1016/j.ijinfomgt.2022.102594

Suryono, R. R., Budi, I., & Purwandari, B. (2020). Challenges and trends of financial technology (Fintech): A systematic literature review. *Information*, *11*(12), 590. https://doi.org/10.3390/info11120590

Tay, L. Y., Tai, H. T., & Tan, G. S. (2022). Digital financial inclusion: A gateway to sustainable development. *Heliyon*, *8*(6), e09766. https://doi.org/10.1016/j.heliyon.2022.e09766

Tut, D. (2023). FinTech and the COVID-19 pandemic: Evidence from electronic payment systems. *Emerging Markets Review*, *54*, 100999. https://doi.org/10.1016/j.ememar.2022.100999

Zhao, Y., Bacao, F., & Dinardo, J. (2020). Bank loan default prediction with machine learning. *Sustainability*, *12*(18), 7708. https://doi.org/10.3390/su12187708