

ORIGINAL RESEARCH

Open access

Digital Payment Dependence in Online Business Ecosystems: A Model of Transaction Control, Customer Friction, and Revenue Vulnerability

Olivia Bennett^{1*}, Harry Collins², Amelia Price¹, Jack Foster²

Abstract

Online businesses increasingly rely on third-party digital payment providers to process customer payments, authenticate transactions, manage settlement, handle disputes, and enable scalable digital commerce. This reliance is often treated as a technical or operational arrangement rather than as a strategic dependency embedded in the firm's revenue architecture. Yet payment dependence can shape how firms access transaction data, control customer experience, manage cash flow, and respond to disruptions.

The central problem addressed in this article is that digital payment providers simultaneously enable and constrain online business ecosystems. They make commerce faster, more secure, and more scalable, but they also introduce external control points into the customer journey and revenue process. When these control points are poorly governed, firms may experience reduced transaction visibility, checkout friction, settlement uncertainty, and exposure to provider decisions.

This article proposes the Digital Payment Dependence Model as an original conceptual framework for understanding how dependence on external payment infrastructures creates three interconnected strategic risks. These are loss of transaction control, customer friction at checkout, and revenue vulnerability. The model explains how these risks reinforce one another and why payment dependence should be treated as a managerial concern rather than a back-office technology issue.

The proposed model contributes to digital business and payment systems research by reframing payment infrastructure as a strategic dependency within online business ecosystems. It shows that payment governance is not limited to transaction fees or technical uptime, but extends to control, experience design, and revenue continuity. The article concludes that managers should govern payment systems as strategic assets whose failure, concentration, or misalignment can directly threaten business resilience.

Keywords Conceptual model, Digital payment dependence, Transaction control, Customer friction, Revenue vulnerability, Online business ecosystems

*Correspondence:

Olivia Bennett
olivia.bennett@bristol.ac.uk

¹ Department of Digital Management and Business Systems, Faculty of Business, University of Bristol, Bristol, United Kingdom

² Department of Strategic Analytics, Faculty of Economics, Durham University, Durham, United Kingdom

Introduction

Digital payment providers have become deeply embedded in online business ecosystems because they allow firms to accept payments across cards, wallets, mobile applications, and platform-mediated checkout environments. Research on digital payments shows that adoption is shaped by perceived convenience, trust, security, and the ability of providers to reduce transaction complexity for both customers and merchants [1]. This integration makes external payment systems appear seamless, but the apparent simplicity of checkout often conceals a complex infrastructure of gateways, processors, wallet providers, risk controls, authentication procedures, and settlement rules. The managerial challenge is that the more seamless this infrastructure becomes, the easier it is for firms to overlook the dependence that supports their revenue collection.

Payment partners enable online businesses to scale faster than they could through internally built payment capabilities alone, especially when firms need cross-border acceptance, fraud protection, and compatibility with diverse customer payment preferences. Studies of mobile payment and wallet adoption demonstrate that provider reputation, perceived trust, privacy, and convenience influence both customer and merchant willingness to transact digitally [2-4]. However, the same providers that enable transactions also shape transaction flow, customer interface design, data access, dispute handling, and settlement timing. This creates a strategic puzzle: payment partners facilitate sales while simultaneously becoming external control points within the firm's value-capture process.

Existing research has produced valuable insights into digital payment adoption, online shopping convenience, mobile wallet use, and e-commerce trust, but these strands remain insufficiently integrated from a strategic risk perspective. For example, studies on checkout abandonment show that friction during the online purchase journey can weaken conversion, while platform research highlights how dependence on external infrastructures can produce power asymmetries and lock-in [5-7]. What remains underdeveloped is a conceptual account of how payment infrastructure dependence links operational payment control, customer experience, and revenue exposure. This article addresses that gap by positioning digital payment dependence as a distinct business problem in online ecosystems.

The aim of this article is to develop the Digital Payment Dependence Model, a conceptual model explaining how reliance on third-party payment infrastructures generates three interconnected dimensions of risk. The first dimension is loss of transaction control, where firms become dependent on provider rules, data structures, settlement processes, and contractual terms. The second is customer friction, where payment flows introduce barriers that affect conversion and customer experience; the third is revenue vulnerability, where provider disruption, concentration, or policy change threatens income continuity [8-10]. By linking these dimensions, the article reframes payment infrastructure as a strategic management issue rather than a narrow technical service.

Digital Payment Dependence as a Business Problem

Digital payment dependence refers to the reliance of an online business on external payment providers to process, authenticate, hold, route, and settle customer payments. This dependence includes payment gateways, card processors, digital wallets, mobile payment platforms, fraud screening systems, and platform-controlled checkout flows. Research on mobile payment adoption shows that such systems are attractive because they reduce transaction effort and create perceived convenience, but they also require firms and consumers to trust external intermediaries with sensitive financial interactions [11, 12]. Dependence therefore begins as a solution to payment complexity but can evolve into a structural reliance on external infrastructure.

The business problem emerges because payment infrastructure is directly connected to revenue capture, not merely to operational support. When a firm depends on an external provider for payment authorization and settlement, the provider becomes part of the firm's revenue architecture and customer interface. Studies of merchant adoption indicate that payment acceptance decisions are shaped by trust, perceived risk, provider capabilities, and the practical constraints faced by merchants [3, 13]. These findings suggest that payment dependence is not neutral: it reflects the distribution of power, information, and operational flexibility between the business and its payment intermediaries.

Digital payment dependence is strategically important because it may reduce a firm's ability to manage customer relationships directly. Payment providers can influence which payment methods are available, how authentication is presented, what data are visible, and how disputes are resolved. Research on digital wallets and QR-code payment systems shows that customers increasingly experience payment providers as part of the retail interface, meaning that provider design choices can shape the perceived quality of the transaction itself [14, 15]. This makes payment dependence especially significant in online ecosystems where checkout is often the final point at which customer intention becomes revenue.

The three core dimensions of the problem are loss of transaction control, customer friction, and revenue vulnerability. Loss of transaction control concerns the firm's reduced authority over payment data, settlement timing, and transaction rules; customer friction concerns the barriers introduced by payment flows; and revenue vulnerability concerns exposure to disruptions, policy changes, fees, holds, or provider withdrawal. Platform dependence research indicates that firms relying on external platforms may face power asymmetries and strategic constraints even when platform participation initially supports growth [6, 7]. Digital payment dependence applies this logic to the payment layer of online commerce, where dependence affects not only visibility but also cash flow and conversion.

Transaction Control and Payment Infrastructure

Transaction control is the managerial capacity to observe, configure, govern, and intervene in the payment process that converts customer intent into realised revenue. In digital payment ecosystems, this control is partly transferred to gateways, processors, wallet providers, and platform checkout systems. Research on digital payment and banking adoption shows that trust, perceived security, and convenience are central to user acceptance, but these same qualities often depend on provider-controlled systems outside the merchant's direct authority [1, 16]. The implication is that transaction control becomes distributed across the business and its external payment partners.

A first control issue concerns data visibility and ownership. Payment providers may supply dashboards, summaries, fraud indicators, and settlement reports, but firms may not receive full access to transaction-level data, authentication signals, failure reasons, or customer payment preferences. Studies of e-commerce trust and mobile application customer experience show that data-mediated interactions shape customer confidence and service quality, yet firms often depend on external systems to generate and interpret those interactions [17, 18]. When payment data are incomplete or provider-defined, managers may struggle to understand why customers abandon checkout, experience declines, or face authentication problems.

A second control issue concerns contractual leverage and settlement authority. Payment providers can impose fee schedules, reserve requirements, dispute procedures, account reviews, and settlement timelines that affect cash flow and operating flexibility. Research on third-party payment platform risk highlights that these intermediaries can introduce operational and governance risks through their control over platform rules, security procedures, and transaction handling [19]. For smaller online firms, the asymmetry can be especially acute because the business may depend on the provider's infrastructure but lack the bargaining power to customise terms or negotiate exceptions.

A third control issue concerns the design of the payment flow itself, including redirects, embedded checkout screens, authentication steps, wallet prompts, and payment-method availability. Customer experience research shows that convenience and continuity influence online satisfaction, while cart abandonment research demonstrates that disruptions in the shopping journey can weaken purchase completion [8, 20]. In this sense, transaction control is not merely about back-end processing; it also includes the ability to design a low-friction, trustworthy, and brand-consistent payment experience. Table 1 outlines the dimensions of transaction control affected by digital payment dependence.

Table 1. Transaction Control Dimensions in Digital Payment Dependence: Ownership, Visibility, and Contractual Leverage

Transaction control dimension	How payment dependence weakens managerial control	Strategic consequence for online businesses	Relevant managerial question
Transaction data ownership	Customer payment data, decline reasons, authentication signals, dispute records, and wallet-specific behavioural data may remain partly controlled or filtered by the provider.	The firm has limited ability to diagnose payment failure, personalise checkout recovery, or build independent customer payment intelligence.	Does the firm receive enough transaction-level data to understand payment success, failure, fraud review, and customer payment preference patterns?
Payment-flow visibility	Redirects, wallet screens, processor rules, and authentication layers may occur outside the firm's fully observable interface.	Managers may misinterpret checkout abandonment as general customer disinterest rather than as payment-stage friction or technical failure.	Can the firm identify exactly where in the payment journey customers abandon, fail authentication, or switch payment method?
Settlement control	Settlement timing, reserve policies, chargeback deductions, rolling holds, and payout interruptions may be determined by the provider.	Cash-flow planning becomes vulnerable to external rules, creating liquidity pressure when revenue is delayed or withheld.	How dependent is operating cash flow on the provider's payout schedule, reserve policy, and dispute-management process?
Contractual leverage	Providers may alter pricing, acceptable-use rules, service terms, risk thresholds, or dispute processes with limited negotiation space for the merchant.	The business may face rising costs or reduced service access without sufficient ability to renegotiate or switch quickly.	Does the firm have contractual protections, escalation routes, and realistic alternatives if provider terms change?
Payment-method configuration	The provider may limit available cards, wallets, currencies, local payment methods, or alternative transaction routes.	The firm may lose customers whose preferred payment methods are unavailable or poorly integrated.	Are payment methods selected according to customer needs, geographic markets, and conversion data rather than provider convenience alone?
Dispute and chargeback governance	Chargeback evidence formats, dispute windows, fraud rules, and appeal procedures may be provider-defined.	The firm may lose revenue or customer goodwill when disputes cannot be managed with sufficient transparency or flexibility.	Can managers trace, contest, and learn from disputes in ways that improve both fraud control and customer service?

Customer Friction and Checkout Failure

Customer friction occurs when the payment stage interrupts the customer's movement from purchase intention to completed transaction. Digital payment studies show that customers value convenience, trust, privacy, and perceived control, but these expectations can be weakened when payment flows require excessive authentication, account creation, redirection, or unfamiliar wallet interfaces [4, 21]. In online business ecosystems, friction is especially damaging because the checkout stage is not merely a technical endpoint but the moment at which customer motivation must be converted into revenue. A payment provider that improves security while increasing complexity can therefore create a tension between risk control and conversion performance.

Payment-method fit is a central source of friction because customers differ in their preferred instruments, habits, and expectations. Research on payment choice shows that transaction characteristics influence how consumers select payment methods, while low-income and digitally constrained consumers may respond differently to payment formats and perceived payment effort [22, 23]. If an online business depends on a provider that does not support locally preferred methods, instalment options, digital wallets, or low-friction mobile flows, the firm may unintentionally exclude otherwise willing buyers. This converts payment dependence into a market-access problem rather than only a checkout-design problem.

Technical and procedural failures also contribute to checkout abandonment. Cart abandonment research shows that customers may withdraw when the online purchase journey becomes confusing, risky, inconvenient, or misaligned with their expectations [5, 20]. More recent work on cart abandonment further indicates that perceived risk and confusion can mediate the relationship between online information environments and abandonment behaviour [24]. When payment failures are opaque, customers may not know whether the problem lies with their bank, the merchant, the payment provider, authentication rules, or a temporary system fault.

The long-term effect of checkout friction is not limited to a single lost transaction. Mobile payment research indicates that continuous use depends on initial trust, perceived reliability, value, and customer involvement, which means that repeated payment problems can weaken future willingness to return [16, 21]. For online businesses, this creates a conversion-retention link: friction at checkout reduces immediate sales while also damaging customer lifetime value. Digital payment dependence therefore shapes both transactional performance and relationship quality.

Revenue Vulnerability in Online Business Ecosystems

Revenue vulnerability refers to the exposure of online businesses to interruptions, delays, cost increases, or access restrictions in the payment infrastructure through which income is collected. Third-party payment platforms can improve efficiency and scalability, but they also create operational risk when firms rely on them for authorisation, settlement, fraud control, dispute handling, and compliance screening [19]. The vulnerability is especially acute because payment infrastructure is directly connected to cash inflow. If the payment layer fails, the business may continue to generate customer demand while being unable to convert that demand into usable revenue.

One source of vulnerability is settlement uncertainty. Payment providers may delay payouts, hold funds, deduct chargebacks, apply reserves, or subject transactions to risk review before funds become available to the merchant. Studies of digital payment systems and consumer experience highlight the importance of reliability, security, and trust in sustaining payment use, yet these same safeguards can create cash-flow constraints when provider risk controls override merchant expectations [25, 26]. In this sense, protection mechanisms designed for system integrity may also increase business exposure when they are opaque, slow, or difficult to contest.

A second source is concentration risk. If a firm depends heavily on a single payment provider, a provider outage, policy change, fee increase, account suspension, or de-platforming event can disrupt revenue capture across the whole business. Platform dependence research shows that firms operating through external digital infrastructures face power asymmetries and strategic risks because critical rules may be controlled outside the firm [7, 8]. Payment dependence intensifies this problem because the affected asset is not only visibility or market access but the firm's ability to receive money from customers.

Revenue vulnerability is aggravated when firms lack fallback payment routes, direct banking relationships, alternative invoicing options, or internal knowledge of payment operations. Digital transformation research emphasises that digital business innovation creates new opportunities but also new dependencies, governance challenges, and organisational capability requirements [27]. For payment-dependent firms, the relevant managerial issue is whether payment infrastructure has been governed as a resilience-critical system. **Table 2** categorises sources and consequences of revenue vulnerability from payment dependence.

Table 2. Revenue Vulnerability from Digital Payment Dependence: Risk Sources, Financial Impact, and Aggravating Factors

Revenue vulnerability source	How the vulnerability emerges	Direct financial impact	Aggravating factors	Managerial implication
Provider outage	The payment gateway, processor, wallet, or authentication layer becomes unavailable during trading periods.	Lost sales, failed subscriptions, delayed renewals, and increased customer-service costs.	Single-provider dependence, no offline fallback, weak monitoring, and lack of rapid customer communication.	Treat payment uptime as a revenue-continuity metric rather than only an IT performance measure.
Funds hold or rolling reserve	The provider delays or withholds payouts because of perceived risk, disputes, chargeback ratios, or policy triggers.	Liquidity pressure, delayed supplier payments, payroll stress, and reduced working-capital flexibility.	High transaction volume volatility, limited cash buffer, weak dispute evidence, and unclear reserve clauses.	Negotiate settlement transparency and maintain cash-flow buffers linked to payment risk exposure.
Fee increase	The provider changes transaction fees, currency-conversion costs, dispute charges, or premium-service pricing.	Margin erosion, pricing pressure, and reduced profitability in low-margin online segments.	Low bargaining power, lack of competing providers, complex cross-border payment mix, and limited pricing flexibility.	Model fee sensitivity and maintain provider alternatives before pricing pressure becomes urgent.
Chargeback exposure	Provider-controlled dispute rules determine evidence requirements, timelines, and liability allocation.	Revenue reversal, dispute fees, inventory loss, and fraud-management costs.	Digital goods, weak proof of delivery, poor customer communication, and high-risk categories.	Integrate payment dispute data into fraud, service, and customer-experience governance.
De-platforming or account suspension	The provider withdraws service access because of risk review, acceptable-use rules, compliance concerns, or policy interpretation.	Sudden inability to accept payments, revenue interruption, reputational damage, and emergency switching costs.	Provider concentration, unclear compliance documentation, weak escalation channels, and absence of backup payment rails.	Build contingency payment routes and monitor provider-rule exposure as a strategic risk.
Limited payment-method coverage	The provider fails to support payment options expected in specific markets or customer segments.	Lower conversion, reduced geographic expansion, and missed revenue from otherwise willing customers.	International growth, mobile-first customers, local wallet preferences, and weak localisation strategy.	Align payment-method portfolio with customer behaviour and market-entry strategy.

Proposed Digital Payment Dependence Model

The Digital Payment Dependence Model proposes that reliance on external payment providers generates revenue vulnerability through two primary pathways: loss of transaction control and customer friction. Loss of transaction control occurs when the firm has limited authority over data access, payment-flow design, settlement timing, dispute procedures, or provider terms. Customer friction occurs when the payment experience becomes inconvenient, uncertain, restrictive, or technically unreliable. Together, these pathways explain why payment dependence should be analysed as a strategic risk system rather than as a narrow processing arrangement [1, 9, 19].

The first pathway moves from dependence to control loss and then to vulnerability. When payment providers intermediate data, authentication, settlement, and dispute governance, managers may be unable to diagnose transaction failures, forecast cash flow accurately, or respond quickly to provider changes [17, 18]. This control loss becomes revenue vulnerability when the firm cannot prevent payment interruption, negotiate favourable terms, access sufficient transaction intelligence, or redesign payment routes at speed. The pathway is especially relevant for firms whose online revenue is concentrated through a small number of payment intermediaries.

The second pathway moves from dependence to customer friction and then to vulnerability. Payment providers influence the checkout interface through supported methods, wallet prompts, authentication rules, redirects, error messages, and technical reliability. Online shopping research shows that convenience, perceived risk, and customer mindset affect whether shoppers complete or abandon the cart [5, 8, 20]. When provider-controlled payment flows create friction, firms face lost conversion, lower repeat purchase, and weaker customer trust, all of which increase exposure to revenue instability.

The model also includes feedback effects because vulnerability can deepen dependence. A firm experiencing failed payments, declining conversion, or delayed settlement may lack the resources and operational slack needed to redesign payment architecture. Platform and digital entrepreneurship research indicates that firms can become locked into external infrastructures even when dependence produces strategic constraints [6, 7]. Table 3 presents the proposed Digital Payment Dependence Model linking the three dimensions.

Table 3. Digital Payment Dependence Model: Constructs, Causal Pathways, and Feedback Effects

Model construct	Conceptual definition	Main causal mechanism	Expected business outcome	Feedback effect
Digital payment dependence	Reliance on external providers for payment processing, authentication, settlement, dispute handling, wallet access, and transaction data.	The firm embeds third-party payment infrastructure into the core revenue process.	Payment infrastructure becomes strategically central to revenue continuity and customer experience.	Greater dependence may reduce incentives or capacity to build alternative payment routes.
Loss of transaction control	Reduced managerial authority over payment data, payment-flow configuration, settlement timing, contractual terms, and dispute procedures.	Provider rules and systems define what the firm can see, change, negotiate, and contest.	Lower diagnostic capacity, weaker bargaining position, and reduced responsiveness to payment disruption.	Control loss limits the firm's ability to recover when revenue vulnerability materialises.
Customer friction	Checkout barriers arising from authentication steps, redirects, payment-method mismatch, account	Provider-controlled payment design interrupts the customer's path from	Cart abandonment, reduced conversion, lower satisfaction, and weaker customer lifetime value.	Repeated friction damages trust, making future checkout recovery more difficult.

	requirements, errors, or unclear failure messages.	purchase intention to completed transaction.		
Revenue vulnerability	Exposure to revenue loss, cash-flow delay, margin erosion, or service interruption caused by provider disruption, policy change, holds, fees, or de-platforming.	Control loss and friction jointly weaken the firm's ability to convert demand into accessible revenue.	Financial instability, strategic fragility, and dependence on emergency payment solutions.	Revenue stress may prevent investment in diversification or internal capability building.
Moderating conditions	Business size, geographic scope, regulatory environment, product type, transaction volume, and customer payment preferences.	These conditions shape the intensity of dependence and the feasibility of mitigation.	Similar payment architectures may create different risk levels across firms and markets.	Firms in complex markets may become more dependent on specialised providers, increasing switching difficulty.
Managerial mitigation capacity	The firm's ability to audit, diversify, negotiate, monitor, and redesign payment infrastructure.	Governance capabilities convert payment dependence from an unmanaged exposure into a monitored strategic risk.	Improved resilience, lower friction, better data use, and greater revenue continuity.	Strong mitigation capacity weakens the negative feedback loop between vulnerability and dependence.

Figure 1 presents the Digital Payment Dependence Model by showing how reliance on third-party payment infrastructures generates loss of transaction control, customer friction, and revenue vulnerability.

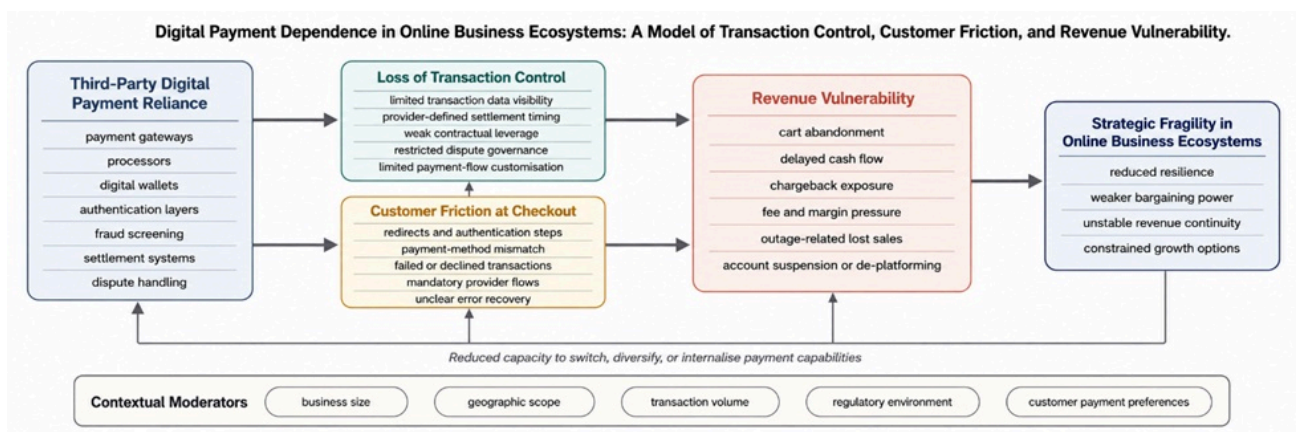


Figure 1. Digital Payment Dependence Model: Pathways from Third-Party Payment Reliance to Transaction Control Loss, Customer Friction, and Revenue Vulnerability

Managerial Response Strategies

The first managerial response is provider diversification. Rather than relying on one gateway, wallet, processor, or platform checkout system, firms can design a layered payment architecture that supports backup routing and market-specific payment options. Research on mobile payments and digital wallet adoption suggests that customers differ in their trust, convenience expectations, and preferred payment instruments, making a single payment route unlikely to serve all

segments equally well [12, 14, 22]. Diversification should therefore be understood not only as risk reduction but also as customer-experience adaptation.

The second response is the development of selective internal payment capabilities. Not every online business can build full payment processing infrastructure, but many firms can strengthen internal competence in payment analytics, chargeback management, failure diagnostics, settlement forecasting, and provider-performance monitoring. Digital transformation research stresses that firms need organisational capabilities to manage digital dependencies, not merely access to external technologies [27]. In payment governance, this means managers should understand how provider rules affect revenue, data, risk, and customer experience.

The third response is payment-friction auditing. Firms should regularly test checkout flows across devices, regions, payment methods, authentication scenarios, failed-payment cases, and returning-customer journeys. Customer experience and cart abandonment research indicates that even small frictions can alter satisfaction and completion behaviour, particularly when customers perceive risk, confusion, or inconvenience [8, 9, 24]. A payment-friction audit should therefore connect technical monitoring with customer journey analysis, revenue analytics, and service recovery design.

Limitations and Future Research

This article is conceptual and does not empirically validate the Digital Payment Dependence Model. Its contribution lies in integrating literature on digital payments, customer experience, e-commerce trust, cart abandonment, and platform dependence into a risk-oriented model of payment dependence. Because the underlying literature includes varied contexts such as mobile wallets, online shopping, platform entrepreneurship, and payment adoption, the model should be treated as a theoretical synthesis requiring future testing [2, 4, 6, 10]. Empirical research could examine whether loss of transaction control and customer friction statistically mediate the relationship between provider dependence and revenue vulnerability.

A second limitation is that the model is primarily oriented toward B2C online business ecosystems. Many of its mechanisms may also apply to B2B commerce, subscription services, marketplaces, digital goods, creator platforms, and cross-border merchants, but these contexts may involve different payment cycles, contract structures, invoicing practices, and settlement risks. Future studies could compare card-based checkout, wallet-based payment, bank transfer, direct debit, and invoice-based payment systems across business models [12, 15, 25]. Such work would clarify whether payment dependence operates differently when the customer is an individual consumer, a platform participant, or an organisational buyer.

A third limitation concerns regulation and emerging payment infrastructures. Regional rules on open banking, consumer authentication, data protection, platform liability, and digital currency may alter how payment dependence is distributed across firms, providers, banks, and regulators. Future research should examine whether central bank digital currencies, account-to-account payment systems, embedded finance, and multi-provider orchestration reduce dependence or simply shift it to new intermediaries [26, 28]. Longitudinal studies would be especially useful for understanding how firms adapt after outages, fee changes, funds holds, or provider withdrawal.

Conclusion

This article proposed the Digital Payment Dependence Model to explain how reliance on third-party payment providers creates interconnected risks in online business ecosystems. The model shows that digital payment dependence is not merely a matter of transaction cost or technical convenience. It is a strategic condition that shapes transaction control, checkout experience, and revenue continuity.

The central contribution is to connect loss of transaction control, customer friction, and revenue vulnerability into one coherent conceptual model. Payment providers enable online commerce, but they can also become external control points over data visibility, payment-flow design, settlement timing, dispute procedures, and revenue access. Managers should therefore treat payment infrastructure as a strategic asset and resilience-critical capability rather than as a background utility.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 25 May 2026

Revised: 10 Jul 2026

Accepted: 20 Aug 2026

Published online: 18 September 2026

Rights and permissions

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Alkhowaiter WA. Digital payment and banking adoption research in Gulf countries: A systematic literature review. *Int J Inf Manag.* 2020;53:102102.
- Cardoso S, Martinez LF. Online payments strategy: How third-party internet seals of approval and payment provider reputation influence the Millennials' online transactions. *Electron Commer Res.* 2019;19(1):189-209.
- Singh N, Sinha N. How perceived trust mediates merchant's intention to use a mobile wallet technology. *J Retail Consum Serv.* 2020;52:101894.

- Mombeuil C, Uhde H. Relative convenience, relative advantage, perceived security, perceived privacy, and continuous use intention of China's WeChat Pay: A mixed-method two-phase design study. *J Retail Consum Serv.* 2021;59:102384.
- Kapoor AP, Vij M. Following you wherever you go: Mobile shopping 'cart-checkout' abandonment. *J Retail Consum Serv.* 2021;61:102553.
- De Reuver M, Sørensen C, Basole RC. The digital platform: A research agenda. *J Inf Technol.* 2018;33(2):124-35.
- Cutolo D, Kenney M. Platform-dependent entrepreneurs: Power asymmetries, risks, and strategies in the platform economy. *Acad Manag Perspect.* 2021;35(4):584-605.
- Duarte P, e Silva SC, Ferreira MB. How convenient is it? Delivering online shopping convenience to enhance customer satisfaction and encourage e-WOM. *J Retail Consum Serv.* 2018;44:161-9.
- Mittal B. The psychology of online shopping cart abandonment: A scrutiny of the current research framework and building an improved model of the online shopper journey. *Electron Commer Res.* 2025;25(2):777-803.
- Ciaburri M, Savio R, Ferri S, Tiscini R. E-commerce platform dependence: A double-edged sword for born global firms?. *Int Entrep Manag J.* 2026;22(2):76.
- Kaur P, Dhir A, Singh N, Sahu G, Almotairi M. An innovation resistance theory perspective on mobile payment solutions. *J Retail Consum Serv.* 2020;55:102059.
- Kaur P, Dhir A, Bodhi R, Singh T, Almotairi M. Why do people use and recommend m-wallets?. *J Retail Consum Serv.* 2020;56:102091.
- Moghavvemi S, Mei TX, Phoong SW, Phoong SY. Drivers and barriers of mobile payment adoption: Malaysian merchants' perspective. *J Retail Consum Serv.* 2021;59:102364.
- Yan LY, Tan GW, Loh XM, Hew JJ, Ooi KB. QR code and mobile payment: The disruptive forces in retail. *J Retail Consum Serv.* 2021;58:102300.
- Liao SH, Yang LL. Mobile payment and online to offline retail business models. *J Retail Consum Serv.* 2020;57:102230.
- Talwar S, Dhir A, Khalil A, Mohan G, Islam AN. Point of adoption and beyond. Initial trust and mobile-payment continuation intention. *J Retail Consum Serv.* 2020;55:102086.
- Oliveira T, Alinho M, Rita P, Dhillon G. Modelling and testing consumer trust dimensions in e-commerce. *Comput Hum Behav.* 2017;71:153-64.
- McLean G, Al-Nabhani K, Wilson A. Developing a mobile applications customer experience model (MACE)-implications for retailers. *J Bus Res.* 2018;85:325-36.
- Yao Y, Li J. Operational risk assessment of third-party payment platforms: A case study of China. *Financ Innov.* 2022;8(1):19.
- Rubin D, Martins C, Ilyuk V, Hildebrand D. Online shopping cart abandonment: a consumer mindset perspective. *J Consum Mark.* 2020;37(5):487-99.
- Chakraborty D, Siddiqui A, Siddiqui M, Rana NP, Dash G. Mobile payment apps filling value gaps: Integrating consumption values with initial trust and customer involvement. *J Retail Consum Serv.* 2022;66:102946.
- Świecka B, Terefenko P, Paprotny D. Transaction factors' influence on the choice of payment by Polish consumers. *J Retail Consum Serv.* 2021;58:102264.

Greenacre L, Akbar S. The impact of payment method on shopping behaviour among low income consumers. *J Retail Consum Serv.* 2019;47:87-93.

Roy R, Shaikh A. The impact of online consumer review confusion on online shopping cart abandonment: A mediating role of perceived risk and moderating role of mindfulness. *J Retail Consum Serv.* 2024;81:103941.

Shree S, Pratap B, Saroy R, Dhal S. Digital payments and consumer experience in India: a survey based empirical study. *J Bank Financ Technol.* 2021;5(1):1-20.

Hwang Y, Park S, Shin N. Sustainable development of a mobile payment security environment using fintech solutions. *Sustainability.* 2021;13(15):8375.

Nambisan S, Wright M, Feldman M. The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes. *Res Policy.* 2019;48(8):103773.

Verkijika SF, Neneh BN. Standing up for or against: A text-mining study on the recommendation of mobile payment apps. *J Retail Consum Serv.* 2021;63:102743.