Palestine Economic Policy Research Institute (MAS)

معهد ابحاث السياسات الاقتصادية الفلسطيني (ماس)

Technical and Legal Expert Paper

for the National Awareness Campaign on E-Commerce, Digital Marketing, and E-Payments in Palestine

2026

Technical and Legal Expert Paper for the National Awareness Campaign on E-Commerce, Digital Marketing, and E-Payments in Palestine

Main Researcher: Suhaib Sharif

Assistant Researchers: Zein Omar Hamayel
Nuha Zraiq

Project Coordinator: Raheeq Hurani

This paper was prepared by the Palestine Economic Policy Research Institute (MAS) in partnership with Global Communities (GC) as part of the Supporting MSMEs' Growth and Competitiveness in Palestine Programme (SMCGP), funded by the Swedish Government. The views and opinions expressed in this paper are those of the author and do not necessarily reflect the positions of MAS, Global Communities, or the Swedish Government.

MAS
Palestine Economic Policy Research Institute (MAS)

Palestine Economic Policy Research Institute (MAS)
Jerusalem and Ramallah

Foreword

This paper is the third research output prepared as part of the National Awareness Campaign on E-Commerce, Digital Marketing, and E-Payments in Palestine, implemented by the Palestine Economic Policy Research Institute (MAS) under the Supporting MSMEs' Growth and Competitiveness in Palestine Programme (SMCGP).

Developed by legal expert Suhaib Sharif, the paper aims to provide an analytical overview of the existing legal and regulatory framework governing e-commerce, digital payments, and consumer protection in Palestine. It highlights institutional mandates, enforcement challenges, and opportunities for reform to strengthen trust in digital transactions.

The paper draws upon a focused review of primary legal sources, consultations with relevant stakeholders, and qualitative insights gathered from focus group discussions held with MSMEs in the West Bank. These findings help contextualize the legal analysis with real user experiences and practical implementation gaps. The paper provides a concise, evidence-based, and professionally informed assessment of the current enabling environment and proposes realistic legal and procedural reforms.

We extend our sincere appreciation to our partners, Global Communities (GC) and the Swedish Government, for their support of this project. We also wish to thank the researcher for his valuable efforts and contributions.

Feras Milhem
Director General

Table of Contents

Executive Summary

This technical expert review offers an analytical overview of Palestine's legal and regulatory framework for e-commerce, digital payments, and consumer protection. It identifies the key challenges and institutional responsibilities that shape this framework, and sets out reform priorities to strengthen public trust in digital transactions.

Over the past three years, Palestine has made notable progress in developing the legal framework of its digital economy. National Payment Decree No. 41 of 2022, Decree No. 17 of 2024 on Electronic Transactions and Trust Services, and Decree No. 21 of 2025 on E-Commerce provide a broad framework for regulating online commercial activity and digital payment systems. This corpus validates the legality of electronic contracts, signatures, and records, vests certain powers and responsibilities in the Palestine Monetary Authority (PMA) and the Ministry of National Economy (MoNE) for licensing, oversight, and consumer protection, and establishes the supervisory authority for trust service providers.

While Palestine's digital economy has advanced significantly since the World Bank's 2021 digital economy assessment, external and institutional barriers persist.[1] Connectivity constraints—imposed by the persistent Israeli control over telecommunications infrastructure and spectrum allocation—limit network expansion and access to advanced digital services. Domestically, internal challenges, including the lack of a data protection law and weak coordination among regulatory bodies, continue to hinder digital inclusion and the effective implementation of these developments. Many consumers and micro, small, and medium-sized enterprises (MSMEs) still rely on cash transactions due to fragile trust, limited access to redress mechanisms, and a lack of clarity about how online transactions are safeguarded. Strengthening institutional coordination among the MoNE, PMA, and the Palestine Capital Market Authority (PCMA)—alongside the Consumer Protection Council (CPC)—is essential to ensure a unified approach to market conduct, public communication, and dispute resolution across digital channels. The paper highlights that the success of digital transformation depends on strengthening legal certainty and building public trust, so that consumers and businesses can be confident that online transactions are secure, effective, and protected by clear legal safeguards. The main challenge, however, lies in implementing these recently adopted legal and institutional frameworks. The table below outlines the most significant gaps identified and the corresponding proposed solutions.

Key Gap	Recommended Action
Palestine has a coherent, modern legislative framework for e-commerce, electronic transactions, and digital payments. However, the effectiveness of these laws is constrained by implementation gaps, limited institutional readiness, and market conditions.	Support market readiness through targeted awareness campaigns; MSME onboarding; financial literacy; and practical tools aligned with legal reforms and responsive to business needs.
PMA's digital payment infrastructure is fully operational and stands as the strongest component of the digital economy, but its impact is constrained by international payment restrictions and domestic barriers (e.g., tax clearance invoice limits, high fees, and uneven consumer and MSME readiness).	Address structural barriers to formalization by revising tax clearance invoice thresholds and establishing a mechanism to allow verified digital advertising costs as deductible expenses for tax purposes (currently nondeductible under tax clearance rules).
MSMEs face structural and behavioral barriers, low trust in digital payments, limited international market access, high operating costs, restrictive tax clearance procedures, and the lack of regulated digital platforms or cluster mechanisms that protect their rights.	Enable international market access for Palestinian MSMEs by expanding cross-border payment solutions, forging partnerships to open international payment channels, and guiding MSMEs on participation in global e-commerce platforms. Enhance online intellectual property protection by developing guidance and enforcement mechanisms to

[1] World Bank Group, *Palestinian Digital Economy Assessment* (World Bank, 2021), https://tinyurl.com/bdnc9c2s.

Key Gap	Recommended Action
	address digital copying, trademark misuse, and the sale of counterfeit goods online.
Decree No. 17 of 2024 on Electronic Transactions and Trust Services remains largely inactive because no supervisory authority or trust services infrastructure is in place, limiting the use of legally recognized e-signatures and authenticated digital records.	Activate the decree by appointing the supervisory authority; issuing licensing procedures for Trust Service Providers (TSPs); and establishing a national certification infrastructure for e-signatures and digital identity.
Decree No. 21 of 2025 on E-Commerce requires implementing regulations, templates, and clear procedures, especially to set out obligations for micro and home-based sellers, clarify registration requirements, and balance compliance with business constraints.	Issue implementing regulations under Decree No. 21 of 2025, including clear registration categories; size-specific compliance obligations; and standard templates for terms and conditions, return policies, privacy notices, and complaint procedures.
Data protection and digital consumer rights remain underregulated, undermining public trust in online transactions. The lack of a stand-alone data protection law leaves major gaps in privacy protections, breach notification, and cross-border data processing.	Enact a comprehensive data protection law that provides clear rules on consent, data storage, breach notification, and cross-border data transfers to strengthen trust in online transactions.
Interagency coordination among MoNE, PMA, PCMA, and other stakeholders remains limited, weakening the clarity and consistency of oversight, enforcement, and public communication in the digital market.	Strengthen institutional coordination and establish a single digital dispute resolution channel, jointly managed by MoNE, PMA, and the CPC, with clear timelines and accessible procedures for merchants and consumers.

Taken together, closing these gaps would give consumers and businesses the confidence to treat online transactions as a secure, effective, and legally protected alternative to cash.

1. Introduction

1.1 Background and Context

Palestine has moved gradually toward a digital economy, in which commercial and financial activity increasingly relies on digital technologies, online platforms, and electronic payment systems—a shift that has become more visible in recent years.[2] The growing use of mobile wallets, online retail platforms, and digital marketing tools has created new opportunities for MSMEs and consumers to trade, pay, and connect more efficiently. These developments reflect a growing institutional focus on e-commerce, e-payments, and online consumer protection. Despite this progress, adoption remains limited due to low trust, legal uncertainty, and limited user awareness of rights and obligations in digital transactions.

The digital economy does not operate in isolation from the wider business ecosystem. Its effectiveness depends on how digital transactions and payment systems are integrated into the broader legal and institutional framework governing business registration, company formation, taxation, and access to the banking system.

Earlier assessments of Palestine's digital readiness, including the Palestine Economic Policy Research Institute (MAS)'s 2018 paper *The Digital Economy in Palestine*, highlighted the country's limited progress toward digital transformation at the time. The paper identified multiple barriers to digitization, including restrictions on information and communication technology (ICT) infrastructure, delays in the rollout of mobile broadband networks, and the lack of clear legal frameworks for e-commerce, payments, and data protection. It also cited low public trust, limited digital literacy, and weak institutional coordination as key obstacles to growth. Since 2022, Palestine has taken gradual steps to address these challenges, leading to a series of legislative reforms between 2022 and 2025 that provide a clearer framework for e-commerce, electronic transactions, and digital payments.

With the adoption of Decree No. 21 of 2025 on E-Commerce, Palestine now has a dedicated legal framework for regulating online commercial activity. The decree defines e-commerce as the buying, selling, marketing, and delivery of goods and services through digital channels, including online platforms and electronic payment systems.[3] It builds on Decree No. 17 of 2024 on Electronic Transactions and Trust Services, which gives legal effect to electronic contracts, records, and signatures, and aligns with relevant international instruments that establish baseline rules for digital transactions in Palestine. The effectiveness of these reforms, however, also depends on the broader business framework, particularly the Companies Law and related registration and commercial regulations, which determine whether businesses can access e-payments, digital platforms, and financial services on a formal basis.

While these developments signal meaningful progress, gaps remain between the legal and institutional framework and the realities of digital commerce and payments. Although Decree No. 17 of 2024 and Decree No. 41 of 2022 enshrine key rights and obligations for digital actors, their impact remains contingent on clear communication, consistent interpretation, and implementation—areas that still require stronger public understanding, business awareness, and institutional coordination.

Accordingly, this paper combines a legal and regulatory review with demand-side insights from MSME focus groups to assess whether recent legal reforms reflect market realities and business practices.

---

2 According to the Organisation for Economic Co-operation (OECD), "the Digital Economy incorporates all economic activity reliant on, or significantly enhanced by the use of digital inputs, including digital technologies, digital infrastructure, digital services and data. It refers to all producers and consumers, including government, that are utilizing these digital inputs in their economic activities." Jay Tikam and Habib Hinn, *Digital Financial Services* Roadmap *to Enhance Financial Inclusion* (Palestine Economic Policy Research Institute (MAS), 2023).

3 State of Palestine, Decree No. 21 of 2025 on E-Commerce, art. 1, *Palestinian Official Gazette*, no. 231 (October 27, 2025): 10, https://tinyurl.com/5cx57pz5.

1.2 The Palestinian Context: Binding Structural Challenges

Any assessment of Palestine's legal framework for the digital economy needs to account for structural and political constraints beyond the Palestinian legislature's control. These constraints limit what domestic law can effectively achieve and should frame both the gap analysis and the recommendations. Key challenges include:

1. Continued Israeli control over telecommunications infrastructure and spectrum allocation limits network expansion and access to advanced digital services.
2. Limited monetary sovereignty, reliance on the Israeli shekel, and restricted access to international payment gateways (e.g., PayPal) disadvantage Palestinian businesses and make cross-border trade more complex and costly.
3. Administered by Israel under the Paris Protocol, the clearance system creates significant administrative and financial constraints on businesses selling into the 1948 territories. Annual invoice caps do not reflect actual trade volumes; as a result, many firms shift to informal practices to avoid delays and disputes.
4. The political split between the West Bank and the Gaza Strip limits the application of the Palestinian Authority (PA)'s laws largely to the West Bank, creating divergent regulatory systems and undermining the development of a unified national digital market.

These constraints mean that some ideal solutions are not feasible in the Palestinian context. The paper, therefore, focuses on recommendations within the PA's jurisdiction, while recognizing that the digital economy's full potential will depend on addressing broader structural challenges.

2. E-Commerce and Digital Payments and Marketing: Legal and Regulatory Framework

2.1 Overview

The legal and regulatory framework for e-commerce, e-transactions, and digital payments in Palestine has developed significantly over the past few years. A set of core instruments now recognizes digital activity and provides a legal basis for online contracting, payments, and consumer protection. These include the decrees on e-transactions and e-commerce—regulations governing payment service providers (PSPs) under PMA supervision; consumer protection legislation; and an emerging data protection framework. Together, these instruments establish the legal validity of electronic transactions and a regulatory framework for payment services, addressing a long-standing gap in the legal recognition of digital transactions and payment services.

Most of these instruments were enacted as decrees under Article 43 of the Amended Basic Law of 2003, a mechanism for cases of necessity when the legislative council is not in session. In practice, the council's prolonged inactivity has meant that key elements of the digital economy framework bypass the ordinary legislative process and then depend on secondary regulations, institutional designation, and administrative guidance to become operational. The result is more uncertainty and less public confidence. Market actors may accept these laws on paper, but trust requires predictable procedures, clear enforcement mechanisms, and institutions that can translate this corpus of laws into protections on the ground.

The effectiveness of this framework is shaped less by individual laws than by how they operate together within the broader business and regulatory ecosystem. The main challenges lie in weak implementation, unclear obligations, and inadequate institutional coordination, especially for informal and semi-informal small and micro enterprises (SMEs). While legislation authorizes digital commerce in principle, its reach is uneven in practice, and enforcement often operates indirectly through banks, PSPs, and payment systems rather than through direct oversight of online activity. This creates a gap between the legal framework and how businesses and consumers experience the digital economy day-to-day.

2.2 Core Digital Economy Legislation

This section outlines the main laws governing e-commerce, e-transactions, digital payments, and other components of the digital economy in Palestine. The following laws, decrees, regulations, and instructions constitute the legal basis for digital activity. Their impact, however, turns on implementation: how the provisions are put into effect, coordinated, and aligned with institutional capacity.

- **Decree No. 17 of 2024 on Electronic Transactions and Trust Services** establishes the legal validity of electronic documents, signatures, and contracts and creates a licensing framework for TSPs to support secure digital authentication. While comprehensive in scope, implementation remains limited because no supervisory authority has been designated, and the trust services infrastructure is not yet operational.
- **National Payment Decree No. 41 of 2022**, together with **PMA regulations and instructions**, establishes a unified framework for electronic payments and places payment systems and providers under PMA supervision, including the licensing of nonbank PSPs.
- **Consumer Protection Law No. 21 of 2005, as amended**, guarantees basic consumer rights, but it predates widespread e-commerce; current amendments would add e-commerce provisions.
- **Decree No. 21 of 2025 on E-Commerce** is the most recent addendum to the digital economy legislation. It regulates online commercial activity and sets standard provisions for digital business,

contracts, and consumer transactions. Its effect depends heavily on the issuance of executive regulations and on the MoNE's capacity to enforce compliance.

- Cybercrime Decree No. 10 of 2018 **criminalizes** offenses involving information systems and electronic data and serves as the backbone of cybersecurity enforcement. It is essential for the deterrence of online fraud and cybercrime, but it focuses on punitive measures rather than prevention and does not impose clear cybersecurity duties on digital businesses.
- Data Protection. Palestine has not adopted a stand-alone data protection law. Although a draft bill has been under discussion for several years, it has not entered into force.
- **Decree No. 11 of 2025 on Competition** establishes a modern framework to prohibit anticompetitive agreements, prevent abuses of dominance, and oversee merger control. Although comprehensive, it remains technology-neutral and lacks provisions on digital markets; e-commerce cases, therefore, are assessed through general competition tools.

This body of legislation aims to provide legal certainty for electronic transactions and payments. Legal certainty alone, however, does not drive uptake: implementation and enforcement determine whether the framework translates into greater public trust—especially among MSMEs and consumers who remain hesitant to shift fully to digital channels. The next subsection presents the main elements of the legal and regulatory framework. Subsequent sections examine each element in greater detail, setting out the key provisions, the practical obstacles to adoption and enforcement, and how the instruments fit within the broader regulatory landscape.

2.2.1 Legal and Regulatory Framework Components

2.2.1.1 Decree No. 17 of 2024 on Electronic Transactions and Trust Services[4]

Scope and Key Provisions

Decree No. 17 of 2024 on Electronic Transactions and Trust Services is Palestine's most comprehensive instrument for governing electronic transactions and establishing a trust services framework. It establishes the legal validity of electronic documents, signatures, records, and seals and accords them the same evidentiary weight as paper-based instruments (arts. 12–20[5], 42–45[6]). It also authorizes secure, verifiable, and efficient electronic communications across the public and private sectors, drawing on international models, including the UNCITRAL Model Law of 2001 on Electronic Signatures.

Decree no. 17 of 2024 applies to most civil and commercial transactions carried out electronically, including electronic contracts, invoices, and business correspondence (art. 3).[7] It expressly excludes personal status matters and real estate transactions, which remain subject to conventional formalities and notarization, given their legal and cultural sensitivity.

Under this decree, transactions carried out through automated systems have legal effect (art. 20).[8] Online platforms and electronic agents may enter into valid contracts if the decree's authenticity and integrity requirements are satisfied.

Institutional Framework and Licensing of Trust Services

Decree No. 17 of 2024 sets up a licensing and oversight regime for TSPs—entities that issue and manage electronic signatures, seals, time stamps, and digital delivery certificates. These services underpin *digital identity* and secure online authentication.

4 State of Palestine, *Decree No. 17 of 2024 on Electronic Transactions and Trust Services*, *Palestinian Official Gazette*, no. 220 (November 25, 2024): 4. https://tinyurl.com/2rkmwb34.

5 Decree No. 17 of 2024, arts. 12–20.

6 Decree No. 17 of 2024, arts. 42–45.

7 Decree No. 17 of 2024, art. 3.

8 Decree No. 17 of 2024, art. 20.

A supervisory authority—still not formally designated—would be responsible for licensing, inspections, and audits, and for ensuring compliance with the decree's technical and security requirements (arts. 10,[9] 26,[10] 30–32,[11] 36–38).

Licensed TSPs are required to:

- Maintain the security and integrity of their systems.
- Publish certification information and keep public registers of trust credentials.
- Report, without undue delay, security incidents that could affect reliability.
- Comply with ongoing audits and renewal requirements.

The decree also provides for enforcement: operating as a TSP without a license, falsifying certification data, or tampering with electronic records constitutes a criminal offense under its penalty provisions.

Legal and Evidentiary Effect

Articles 12–20 and 42–45 of Decree No. 17 of 2024 put electronic signatures on the same legal footing as handwritten signatures. They also confirm that an electronic offer and acceptance, once properly authenticated, are legally binding and admissible in court. Valid electronic signatures and digital seals issued by licensed TSPs carry the same evidentiary effect as conventional documents—a key step in enabling digital contracting and documentation across public procurement, commerce, and finance.

Implementation Challenges

While Decree No. 17 of 2024 sets out a coherent framework for electronic transactions and trust services, its provisions remain inactive due to the absence of institutional and technical infrastructure. The supervisory authority mandated to license and oversee TSPs has not been appointed, and the systems needed to verify digital identity, qualified electronic signatures, and timestamps are not in place. As a result, the effect of the decree remains dormant, and businesses and consumers continue to rely on paper-based processes.

In the meantime, and in the absence of an operational national trust services framework, the PMA's iDplus platform functions as a practical mechanism for electronic customer verification and onboarding in the financial sector. iDplus supports secure electronic know-your-customer procedures (e-KYC) and authenticated access to banking and payment services. From both technical and legal perspectives, it is capable of supporting advanced digital authentication and electronic signature functions.

However, iDplus has not been formally licensed or designated as a national trust service provider under Decree No. 17 of 2024, nor has it been integrated into a national certification infrastructure overseen by a designated supervisory authority. Institutionally confined to regulated financial entities, it has not been extended on a system-wide basis to civil, commercial, or public sector transactions, such as contract execution, notarization, or public service authentication.

This gap in digital identity governance constrains the wider use of e-signatures and e-records across the economy. Businesses cannot yet rely on them for contract execution or document submission; public institutions also remain unable to issue or accept digitally verified documents; and courts lack procedural rules governing the admission of electronic evidence. Until a supervisory authority is designated and a national certification infrastructure is established, e-signatures will remain legally valid but unusable in practice.

The next priority is to bridge this gap through a phased strategy that builds on iDplus as the platform for a national digital identity verification system, issues and operationalizes implementing regulations

---

[9] Decree No. 17 of 2024, art. 10.

[10] Decree No. 17 of 2024, art. 26.

[11] Decree No. 17 of 2024, arts. 30–32.

for trust services, and adopts the technical standards needed for certification and cross-border recognition, consistent with the European Union (EU)'s Electronic Identification, Authentication, and trust Services (eIDAS) framework and relevant UNCITRAL instruments.

2.2.1.2 Decree No. 21 of 2025 on E-Commerce[12]

Decree No. 21 of 2025 on E-Commerce establishes Palestine's first comprehensive legislative framework for e-commerce. It governs commercial activity conducted through digital channels, including online sales, marketing, and delivery of goods and services. Alongside Decree No. 17 of 2024 and Decree No. 41 of 2022, it forms the core legal framework for Palestine's digital economy.

Scope and Key Provisions

Decree No. 21 of 2025 applies to online commercial activity carried out in Palestine by individuals and companies, whether through websites, applications, or social media. It introduces a mandatory Electronic Commerce Register, administered by the MoNE, and requires e-commerce providers to register before commencing operations. Registrants receive an official e-commerce identification number that must be displayed on their platforms and invoices. This enables consumers to verify the legitimacy of online sellers and provides a basis for regulatory oversight.

The decree also sets requirements for electronic contracts. Suppliers must disclose essential information, including their identity, the full price (including taxes), delivery terms, and return or warranty policies, before the contract is concluded. It further bans electronic advertising that contains misleading, fraudulent, or unlawful content, aligning online commerce with the consumer protection principles reflected in Consumer Protection Law No. 21 of 2005.

While Decree No. 21 of 2025 designates the MoNE as the competent authority for regulating and supervising e-commerce, it does not establish, as a matter of law, a specialized or independent body dedicated exclusively to e-commerce oversight. Regulatory, registration, inspection, and enforcement functions, therefore, remain with the MoNE under its existing administrative structure, pending further organization through implementing regulations or internal ministerial arrangements. The effectiveness of this oversight framework depends on the timely issuance of implementing regulations and the development of the MoNE's capacity.

Consumer Rights and Data Obligations

Consumer protection lies at the center of the new framework. The law guarantees consumers the right to accurate information, the right to return or replace nonconforming products within four days, and the right to a refund for delayed or incomplete delivery. It also requires online suppliers to issue electronic invoices and to offer at least one electronic payment option through a PMA-licensed provider, so transactions are securely processed through regulated payment systems.

Article 14 of Decree No. 21 of 2025[13] defines supplier responsibilities for protecting consumers' personal data. Businesses are required to obtain explicit consent before processing sensitive personal information and may not disclose such information to third parties without a legal basis. These safeguards remain limited in scope, however, because Palestine has not enacted a comprehensive data protection law. The absence of detailed rules on breach notification, user rights, and cross-border data transfers leaves significant gaps in enforcement.

Implementation Challenges

Effective implementation hinges on the issuance of executive regulations and instructions by the MoNE to operationalize registration procedures, compliance monitoring, and complaint handling mechanisms. Decree No. 21 of 2025 designates the MoNE as the competent authority for receiving and processing

[12] State of Palestine, *Decree No. 21 of 2025 on E-Commerce*, *Palestinian Official Gazette*, no. 231 (October 27, 2025): 10. https://tinyurl.com/jr7t8nd2.

[13] Decree No. 21 of 2025 on E-Commerce, art. 14.

e-commerce complaints through channels it establishes for this purpose. Coordination with the PMA and the Ministry of Telecommunications and Digital Economy (MTDE) is also critical to prevent regulatory overlap, particularly on licensing, cybersecurity, and technical standards. To date, the Electronic Commerce Register has not been launched, and MSMEs and small online vendors continue to operate informally, especially through social media platforms.

While the decree does not impose specific cybersecurity requirements, cybersecurity may be addressed through complementary instruments (e.g., PMA instructions or a national cybersecurity strategy). Without clear obligations for e-commerce platforms, data security and consumer confidence may remain fragile.

Overall, Decree No. 21 of 2025 is a material step toward formalizing the digital economy. It clarifies the basic rules for online transactions, strengthens consumer protections, and broadly aligns with core elements of the UNCITRAL Model Law on Electronic Commerce, including electronic contracting, mandatory disclosures, and record retention.

2.2.1.3 Consumer Protection Law No. 21 of 2005[14] and Its Amendments[15]

Consumer Protection Law No. 21 of 2005, as amended by Decree No. 27 of 2018, forms the cornerstone of consumer rights legislation in Palestine. Although originally designed for traditional commerce, its provisions extend to e-commerce and digital transactions by promoting fairness, transparency, and accountability in business-to-consumer relationships. The law also establishes the institutional basis for consumer protection through the CPC, operating under the MoNE, and requires suppliers to ensure the quality, safety, and accuracy of goods and services offered to the public.

Scope and Key Provisions
Law No. 21 of 2005 applies to all goods and services marketed or supplied to consumers within Palestine, regardless of medium—physical or digital. It bans deceptive advertising (art. 15),[16] obliges suppliers to clearly disclose prices and contractual terms (arts. 16–17),[17] and grants consumers the right to accurate information, fair treatment, and recourse in cases of harm or misrepresentation (art. 3).[18] Suppliers are also required to issue detailed invoices, provide information in Arabic (art. 12),[19] and recall defective or unsafe products from the market (art. 11).[20]

While this law predates widespread digitization, its principles extend to online trade on the basis that e-commerce is subject to the same consumer protection obligations as offline transactions. Online vendors are therefore expected to comply with the same requirements as offline suppliers, including truth-in-advertising, pricing transparency, and accountability for product quality.

Institutional Roles and Enforcement
The CPC, chaired by MoNE, is responsible for policy formulation, complaint handling, and coordination with other authorities. Enforcement is supported by specialized inspection units that may impose administrative measures or refer cases to courts. However, enforcement remains uneven due to limited resources, unclear jurisdictional boundaries with sector regulators, and the absence of dedicated enforcement mechanisms for digital commerce.

---

14 State of Palestine, *Consumer Protection Law No. 21 of 2005*, *Palestinian Gazette*, no. 63 (April 27, 2006), 29. https://tinyurl.com/jr7t8nd2.

15 State of Palestine, *Decision by Decree No. 27 of 2018, Amending Consumer Protection Law No. 21 of 2005, Palestinian Gazette*, Special Issue no. 18 (July 31, 2018), 40.

16 Consumer Protection Law No. 21 of 2005, art. 15.

17 Consumer Protection Law No. 21 of 2005, arts. 16–17.

18 Consumer Protection Law No. 21 of 2005, art. 3.

19 Consumer Protection Law No. 21 of 2005, art. 12.

20 Consumer Protection Law No. 21 of 2005, art. 11.

In response to these challenges, MoNE is leading an amendment process to modernize the law and align it with an increasingly digital marketplace. The proposed amendments aim to introduce explicit provisions on e-transactions, remote sales, and e-commerce rights, particularly on online contract formation, withdrawal rights, refund procedures, and transparency obligations for digital suppliers. These reforms would better align the legislation with international benchmarks, including the UNCITRAL Model Law on Electronic Commerce and the United Nations Guidelines for Consumer Protection (UNGCP).

Consumer Rights in the Digital Context
Law No. 21 of 2005 affirms core consumer rights, including the right to safety, information, and fair treatment. However, the absence of digital-specific provisions, such as standardized return policies, online complaint channels, and privacy safeguards, limits its effectiveness in e-commerce. The ongoing amendments seek to address these loopholes by ensuring that consumers engaging in e-commerce receive the same protection as those purchasing in physical markets.

In parallel, the PMA's regulations under National Payment Decree No. 41 of 2022 help bridge some of these gaps by mandating transparency, data protection, and dispute resolution measures for digital payment providers. However, coordination between MoNE and the PMA remains essential to avoid regulatory fragmentation and ensure a coherent consumer protection approach.

Law No. 21 of 2005 remains a solid foundation, but it has not yet been fully adapted to e-commerce. Enforcement constraints, institutional overlap, and the absence of digital-specific provisions continue to weaken consumer confidence in online transactions. Once the amendments and implementing regulations are enacted, the law could provide a workable bridge between traditional and digital markets by extending consumer protections across commercial platforms. Further refinement of the legal framework and greater consumer awareness, particularly in the digital context, remain necessary to translate the law's protections into practice.

2.2.1.4 Cybercrime Decree No. 10 of 2018[21]

Decree No. 10 of 2018 establishes a comprehensive legal framework to combat cybercrime in Palestine, criminalizing a wide range of offenses, including unauthorized access to information systems, interference with data, and computer-related fraud. It grants law enforcement agencies significant powers to investigate and prosecute cybercrimes, aligning Palestinian legislation with international standards such as the Budapest Convention on Cybercrime. The law's primary focus is on protecting the integrity, confidentiality, and availability of computer systems and data, which are essential to building a secure digital environment. In practical terms, this means that activities such as hacking, data theft, and online fraud are now subject to criminal penalties, providing a legal deterrent against malicious cyber activities.

The scope of Decree No. 10 of 2018 is extensive, covering offenses against computer systems and data, as well as computer-related crimes. Key provisions include the criminalization of illegal access to information systems (art. 3),[22] illegal interception of data (art. 4),[23] and both data and system interference (arts. 5[24] and 6).[25] These articles are fundamental to protecting the technical infrastructure that underpins electronic transactions and digital services. The law also criminalizes the misuse of devices, such as the creation or distribution of malware (art. 7),[26] and computer-related forgery and fraud

21 State of Palestine, *Decree No. 10 of 2018 on Cybercrime*, Palestinian Gazette, Special Issue no. 16 (May 3, 2018), 8. https://tinyurl.com/mu4hnvaj.

22 Decree No. 10 of 2018 on Cybercrime, art. 3.

23 Decree No. 10 of 2018 on Cybercrime, art. 4.

24 Decree No. 10 of 2018 on Cybercrime, art. 5.

25 Decree No. 10 of 2018 on Cybercrime, art. 6.

26 Decree No. 10 of 2018 on Cybercrime, art. 7.

(arts. 8[27] and 9).[28] These provisions are directly relevant to e-commerce, as they provide a legal basis for prosecuting online scams, phishing attacks, and other forms of digital fraud that can undermine consumer trust.

Central to the decree is its focus on enforcement and punishment. It imposes significant penalties, including imprisonment and fines, for a wide range of cybercrimes. The decree also introduces the concept of liability for legal persons (art. 15),[29] meaning that companies can be held responsible for cybercrimes committed on their behalf. Furthermore, it establishes aggravating circumstances that can lead to increased penalties, such as when an organized criminal group commits an offense or targets critical infrastructure (art. 16[30]). These strong enforcement mechanisms are designed to create a robust deterrent against cybercrime and to ensure that law enforcement has the tools it needs to respond effectively to digital threats.

The decree’s effectiveness, however, depends on its implementation and the justice system's capacity to handle complex cybercrime cases. While the law provides a strong punitive framework, it is less focused on preventive measures, such as mandating security standards for businesses or requiring breach notifications. The law’s privacy provisions are also limited, focusing on criminalizing privacy violations rather than establishing a comprehensive data protection framework. For the law to be truly effective in securing Palestine’s digital future, it must be complemented by efforts to build technical and investigative capacity within law enforcement, raise public awareness of cyber risks, and promote a culture of cybersecurity among businesses and individuals. Decree No. 10 of 2018 is a critical step forward in the fight against cybercrime, but it is only one part of a broader effort to create a safe, secure, and trustworthy digital society.

2.2.1.5 Decree No. 11 of 2025 on Competition

Decree No. 11 of 2025 on Competition establishes the general legal framework for promoting competition and preventing anticompetitive conduct in Palestine. It prohibits restrictive agreements and concerted practices, regulates the abuse of a dominant position, and introduces merger control to avoid market concentration that could harm consumers and MSMEs. Although the decree is technology-neutral, its provisions are relevant to e-commerce and digital payments, where network effects, data advantages, and platform intermediation can accelerate concentration. In practice, applying competition rules to digital markets will require technical market analysis, proactive monitoring, and coordination with sector regulators (including the PMA for payment services and MoNE for market conduct) to address practices such as unfair platform terms, discriminatory access, or exclusionary arrangements.

2.3 Companies Law No. 42 of 2021 and the Digital Economy

Although sector-specific legislation governs e-commerce and electronic payments, the digital economy’s integration into Palestine’s wider business ecosystem is shaped upstream—through the legal framework for company formation and business activity. In this regard, Companies Law No. 42 of 2021 constitutes a central entry point to formal economic participation, as it regulates the legal status of companies and MSMEs, and determines how they interface with the administrative, fiscal, and financial system within which digital commerce operates.

The Companies Law governs the establishment, legal personality, and internal organization of commercial entities, thereby defining the forms through which economic activity may be carried out on a formal basis. By recognizing legal personality and regulating governance, registration, and representation, the law enables businesses to enter into contracts, open bank accounts, and engage with

27 Decree No. 10 of 2018 on Cybercrime, art. 8.

28 Decree No. 10 of 2018 on Cybercrime, art. 9.

29 Decree No. 10 of 2018 on Cybercrime, art. 15.

30 Decree No. 10 of 2018 on Cybercrime, art. 16.

regulated institutions. While the law does not address digital commerce or electronic transactions directly, it provides the legal foundation for participation in regulated markets, including online markets.

The relationship between the Companies Law and Decree No. 21 of 2025 on E-Commerce is therefore indirect but consequential. The e-commerce decree governs online commercial activity, including disclosure obligations, consumer protection, and transaction validity. In contrast, the Companies Law determines the legal and organizational form through which that activity is undertaken. In the absence of explicit linkage mechanisms between the two frameworks, compliance with e-commerce obligations is mediated through company registration, tax status, and access to regulated financial services, rather than solely through the e-commerce decree.

In practice, access to electronic payments and e-transactions is closely linked to tax registration and fiscal compliance, which operate alongside company registration as practical conditions for participation in the formal digital economy. Businesses that are registered under the Companies Law but remain outside the tax system often face constraints in opening business bank accounts, onboarding with licensed PSPs, or issuing compliant invoices. These requirements shape the extent to which businesses can rely on electronic payments and fully integrate into regulated online commerce.

This interaction has direct implications for the effectiveness and enforceability of the e-commerce decree. A significant portion of online commercial activity continues to rely on cash-on-delivery and informal payment arrangements, not because such activity falls outside the scope of the law, but because integration into regulated payment systems entails fiscal and administrative obligations that many small and micro businesses are reluctant or unable to assume. As a result, compliance with digital commerce regulation is primarily driven by financial institutions and PSPs, as regulated intermediaries, rather than through direct oversight of online sellers. The operation of the digital economy framework, therefore, depends on the interaction among company law, tax administration, and financial regulation as a combined system.

Effective implementation of the digital economy legislation discussed below requires coordination among regulators with distinct albeit complementary mandates over payments, market conduct, consumer protection, and digital infrastructure.

2.4 Digital Payments Within the Legal and Institutional Framework

Against this multi-instrument legal framework, which is shaped by multiple intersecting legal instruments, the digital payments sector offers a relatively advanced example of how legal and regulatory provisions are translated into practice. This is largely due to the structured reform agenda led by the PMA, the national institution responsible for regulating and supervising the banking and payments sector. Over the past decade, the PMA has gradually introduced a coherent legal and regulatory ecosystem that governs payment systems, electronic transactions, and emerging digital financial services. This ecosystem seeks to strengthen financial inclusion, protect consumers, and ensure the safety and integrity of the national payments infrastructure.

2.5 Institutional and Regulatory Authorities

The institutional and regulatory landscape governing Palestine’s digital economy involves several authorities with distinct but complementary mandates. The PMA oversees payment systems and digital financial activities; the PCMA regulates nonbank financial activities conducted both offline and online; and the MoNE is responsible for market conduct, consumer protection, and the registration of e-commerce providers. Together, these institutions form a sector-based regulatory framework in which responsibilities are allocated by sector and activity rather than consolidated within a single digital economy authority.

2.5.1 Institutional Mandate Allocation Under the Digital Economy Legal

The table below summarizes institutional roles and key mandate overlaps.

Table 1. Institutional Roles and Areas of Intersections

Function/regulatory area	PMA	MoNE/CPC	PCMA	MTDE
Payment licensing and supervision	Lead: Regulates banks, PSPs, e-money issuers, and clearing and settlement systems.	–	–	–
E-commerce registers and online market conduct	–	Lead: Manages the E-Commerce Register; monitors advertising, pricing, and disclosures; and handles consumer complaints through the CPC.	–	–
Nonbank financial services *(insurance, securities, leasing, mortgages, factoring)*	–	–	Lead: Supervises nonbank financial institutions and online financial products; sets market conduct and disclosure standards; and co-leads financial inclusion with the PMA.	–
Consumer complaints and redress	Receives and resolves complaints related to payments and PSPs.	Handles general market and e-commerce complaints through the CPC.	Resolves complaints related to financial services and investments.	–
Cybersecurity and ICT infrastructure	Issues regulations on IT, risk, and business continuity for financial institutions.	Coordinates consumer-facing data security awareness.	–	Lead: Manages telecommunications spectrum and national ICT infrastructure security.
Data protection and privacy	Sectoral: KYC/AML requirements.	Policy-led until a general data protection law is enacted.	Sectoral: Financial and insurance client data.	Sectoral: Telecommunications operators.

The institutional mapping in Table 1 shows that the digital economy in Palestine is governed by multiple, function-specific regulatory regimes rather than a single, integrated digital economy authority. Market entry and legal personality are shaped through company and tax law; value exchange is regulated through the payments system under the PMA; transaction validity depends on the electronic transactions framework; market conduct and consumer protection fall under MoNE and the CPC; while infrastructure, cybersecurity, and data flows are overseen through separate telecommunications and sectoral regimes.

This distribution of mandates means that no single institution oversees the digital economic life cycle from entry to enforcement. Instead, compliance is enforced indirectly through regulated intermediaries such as banks, PSPs, platforms, and delivery companies. While this model allows each regulator to operate within its statutory competence, it also creates coordination gaps, overlapping enforcement expectations, and fragmented redress mechanisms from the business and consumer perspectives. As a result, the effectiveness of digital economy regulation depends less on the existence of individual laws than on the interaction between institutions, the sequencing of enforcement tools, and the capacity to align regulatory action across these domains.

2.5.2 PMA

2.5.2.1 Legal Basis and Policy Direction

The foundation of the digital payments regime is National Payment Decree No. 41 of 2022, which replaced the earlier 2012 legislation and established the PMA as the competent authority responsible for licensing, regulating, and supervising all payment systems and service providers. The law provides comprehensive recognition of *noncash and electronic payments*, including electronic financial transfers, clearing and settlement operations, and the use of payment instruments issued by licensed entities. It applies to both bank-based and nonbank PSPs. It establishes the legal finality of payment orders (art. 6), ensuring that once a transaction is processed through the system, it cannot be revoked or contested.

2.5.2.2 Licensing and Oversight

The PMA's mandate covers:

- Licensing, regulation, and supervision of payment systems, PSPs, and fintech operators.
- Setting governance and cybersecurity requirements.
- Monitoring AML/CFT compliance through risk-based KYC protocols.
- Operating the national clearing and settlement infrastructure.

All payment companies must obtain prior authorization from the PMA before registering with the MoNE. To protect consumers from insolvency risk, these companies are required to keep customers' money in separate bank accounts that cannot be used for the company's own expenses (art. 9).

Beyond its legal mandate, the PMA has institutionalized its supervisory role through detailed regulatory instructions issued between 2021 and 2025, ensuring consistent application of Decree No. 41 of 2022 across the digital payment ecosystem.

Furthermore, article 5 of the Decree No. 41 of 2022 introduces the concept of a *digital financial identity and an e-KYC registry*, enabling electronic authentication of clients across financial institutions. This facilitates remote onboarding and supports digital inclusion. The iDplus system allows individuals to verify their identity and complete financial transactions electronically, anytime and anywhere, without visiting branches or submitting paper documents. Through *facial recognition technology*, users can securely log in to banking or payment applications, authorize transactions, and update personal data in real time. The iDplus platform represents the practical implementation of article 5, translating its provisions on digital identity and e-KYC into an operational national system managed by the PMA.

2.5.2.3 PMA Regulatory Infrastructure (2022–2025)

Building upon this legal foundation, the PMA issued a series of regulatory instructions between 2022 and 2025 that collectively established the practical and operational backbone of Palestine's digital payments ecosystem. These regulations enabled:

- The entry and licensing of nonbank PSPs and fintech companies, thereby diversifying the financial sector beyond traditional banking institutions.[31]
- The launch of interoperable national payment systems, including the BURAQ Real Time Gross Settlement System, the iBURAQ Instant Payment System (2024) for 24/7 credit transfers, and the E-SADAD National Bill Payment Platform (2024) for electronic bill presentment and settlement.

[31] State of Palestine, National Payment Decree No. 41 of 2022, arts. 1–2.

- The standardization of Quick Response (QR) code payments under unified national specifications (Instruction No. 2 of 2023) allows merchants and consumers to transact seamlessly across different platforms.
- The integration of prepaid cards and electronic wallets under a single regulatory ceiling, facilitating cross-use of payment tools for both individuals and businesses.
- The promotion of merchant acceptance of digital payments and increased interoperability between banks, PSPs, and government services, thereby improving accessibility and efficiency for MSMEs and consumers.
- These reforms have enabled a tiered and regulated market structure in which licensed PSPs, including *Jawwal Pay*, *PalPay*, MaalChat, Fawateercom, and *NeoCash*, now operate alongside banks under the supervision of the PMA. These entities provide a wide range of services, including mobile wallets, merchant payments, bill payments, and person-to-person (P2P) transfers. Their operations are supported by agent networks that extend financial access to unbanked and underserved communities, particularly in rural areas. This has lowered transaction costs by introducing interoperable infrastructure (such as the iBURAQ instant payment system and the E-SADAD bill platform), enabling direct transfers between banks, e-wallets, and billers without intermediary fees.

They have also increased reliability through the PMA's Instruction No. 3 of 2022 on IT Environment and Business Continuity, which requires 24/7 service availability, disaster recovery systems, and redundancy across all licensed payment platforms. Confidence in digital payments has strengthened as a result of new compliance and consumer protection obligations, including the segregation of client funds (Instruction No. 1 of 2023 on E-Money Guarantee Accounts), standardized QR payment acceptance (Instruction No. 2 of 2023), and mandatory disclosure of fees and exchange rates (Instruction No. 2 of 2024 on E-SADAD).

2.5.2.4 Obligations Imposed on PSPs

At the same time, the PMA's framework imposed a comprehensive set of compliance and operational obligations on all licensed institutions. These obligations ensure financial stability, consumer protection, and data integrity within the digital payments ecosystem.
Licensed PSPs are required to:

- Maintain *segregated customer accounts* and *monthly reconciliations* verified by licensed banks.[32]
- Comply with AML/CFT and KYC procedures, and maintain detailed reporting on client transactions, agent activities, and suspicious activity.[33]
- Implement binding consumer protection, data security, and operational continuity obligations.[34]
- Ensure full interoperability with national systems such as iBURAQ and E-SADAD and guarantee continuous service availability (24/7).[35]
- Provide transparent consumer disclosures, including fees, currency conversion rates, and transaction timelines, while maintaining clear complaint handling procedures.[36]

2.5.2.5 Draft Decree on Reducing the Use of Cash (2025)

A proposed *Decree on Reducing the Use of Cash* (2025) is currently under review and represents the next stage in Palestine's digital payments reform agenda. The new draft legislation seeks to accelerate Palestine's transition toward a cash-light economy by requiring that transactions exceeding 20,000 NIS

32 PMA, *Instruction No. 1 of 2023 on E-Money Guarantee Accounts*, art. 4.
33 Instruction No. 1 of 2023, art. 16.
34 PMA, *Instructions No. 7 of 2021 Regarding the Regulation of the Relationship Between Payment Service Companies and Users*, arts. 5, 6, and 12.
35 Instructions No. 1 of 2024 on Instant Credit Transfer, art. 25.
36 Instructions No. 7 of 2021*, arts.* 5, 6, and 12.

be conducted through regulated noncash means such as electronic transfers, cards, or licensed e-wallets, rather than in physical currency.

The law empowers the PMA, in coordination with the Ministry of Finance, to set or adjust cash transaction ceilings, establish exceptions for humanitarian or emergency contexts, and enforce compliance through financial penalties ranging from 5 to 15 percent of the transaction value. It also mandates all public institutions to offer and accept electronic payment channels, ensuring that government transactions model the shift away from cash.

This measure reinforces the PMA's role as the lead institution for financial digitalization and transparency. By restricting the use of high-value cash, it aims to reduce tax evasion and money laundering **risks**, *expand financial inclusion*, and *enhance trust* in formal digital payment systems. At the same time, the law recognizes structural constraints, such as limited network coverage and varying levels of digital readiness, by allowing phased implementation and temporary exemptions.

If implemented effectively, the Decree will consolidate previous reforms into a cohesive national framework linking legislation, infrastructure, and compliance incentives to build a **secure and** transparent digital payments environment across Palestine.

2.5.3 PCMA

Established by Law No. 13 of 2004, the PCMA regulates, supervises, and oversees the securities, insurance, mortgage finance, financial leasing (and factoring) sectors, and protects consumers/investors in those markets. Its remit covers nonbank financial services, complementing the PMA's oversight of banks, money changers, microfinance institutions, payment systems, and PSPs. In digital contexts, PCMA jurisdiction is triggered when financial instruments or nonbank financial products are offered, advertised, or intermediated online (e.g., online investment offerings, insurtech distribution, or crowdfunding). The PCMA has publicly cautioned against unlicensed crowdfunding platforms and clarifies that no approvals have been granted to operate such activity. Coordination with the PMA is formalized through joint financial inclusion workstreams.

Overall, these requirements have introduced higher compliance standards across the digital finance sector, aligning Palestine's payments governance with regional and international best practices. From a policy standpoint, the PMA's achievements provide a solid foundation for digital transformation, but sustaining this progress will require continued investment in interoperability, consumer education, and institutional coordination, particularly with the MoNE and the PCMA, to ensure coherent development of the broader digital financial ecosystem.

2.5.4 MoNE and CPC

MoNE is the competent authority for market conduct and consumer protection in commerce, including online trade. Under the e-commerce Decree, the Ministry is responsible for establishing and administering the Electronic Commerce Register, setting practical procedures for registration and disclosure, and supervising compliance with supplier obligations (including information duties, advertising standards, invoicing, and basic complaint handling). Through the CPC and its inspection directorates, MoNE receives consumer complaints, conducts market inspections, and can impose administrative measures or refer violations to the competent authorities. Effective implementation will depend on internal capacity, digital supervision tools, and coordination with the PMA on e-payment requirements and with MTDE on technical and cybersecurity aspects.

2.5.5 MTDE

MTDE is the lead authority for the telecommunications and digital infrastructure that underpins the digital economy. Its mandate covers spectrum management, regulation of telecom operators, policies affecting connectivity and network quality, and national ICT initiatives that influence the availability and security of digital services. In the context of e-commerce, MTDE's role intersects with platform and data security, technical standards for online services, and national digital identity and infrastructure projects. It is also a key stakeholder for any implementation measures linked to the national domain (domain.ps), hosting arrangements, and broader cybersecurity coordination.

2.6 Comparative Benchmarking: Palestine, Jordan, and Saudi Arabia

A comparison with regional frameworks shows that different policy choices shape how e-commerce is regulated in neighboring jurisdictions. In Jordan, electronic commerce is governed primarily through the Electronic Transactions Law, which provides legal validity for electronic signatures and records, but does not treat the electronic store as a distinct legal category. Online sales are understood as a continuation of traditional commercial activity rather than a separate, regulated field, and obligations relating to disclosures, consumer rights, or platform practices are addressed only through general commercial and consumer protection rules. This approach results in fewer sector-specific obligations and leaves ample room for practice to evolve organically, a model that, while legally less detailed, has proven easier to implement given existing institutional capacities.

Saudi Arabia, by contrast, adopted a specialized regulatory regime that expressly defines the electronic store and sets out clear rules governing advertising, disclosures, returns, and data handling. The Palestinian e-commerce decree draws conceptually from this more structured model by recognizing the electronic service provider as a defined category and by outlining detailed obligations toward consumers. However, unlike Jordan's flexible, technology-neutral framework, the Palestinian and Saudi approaches impose a degree of regulatory specificity that presumes relatively strong institutional capacity, active oversight mechanisms, and a reliable digital payments and trust services infrastructure.

Beyond transaction-specific regulation, comparative gaps are also evident in cross-cutting areas of digital governance, particularly data protection. In contrast to several neighboring jurisdictions, Palestine has not yet adopted a stand-alone data protection law. Issues of privacy and personal data remain governed by fragmented sectoral provisions, including PMA rules on customer information, telecommunications regulations, and general criminal-law protections. Although a draft data protection bill has been under discussion for several years, it has not yet entered into force. By comparison, Jordan's Personal Data Protection Law No. 24 of 2023 and Saudi Arabia's Personal Data Protection Law (Royal Decree No. M/19 of 2021, as amended in 2023) illustrate how comprehensive data protection frameworks have become a standard component of digital economy regulation in the region.

Viewed together, these models illustrate different legislative philosophies: Jordan prioritizes general legal principles and practical feasibility, allowing the market to operate with minimal regulatory intervention, while Saudi Arabia and Palestine opt for a dedicated statutory framework that seeks to organize digital commerce more comprehensively. The Palestinian model, therefore, reflects a policy choice toward specialization, but it also requires administrative, technical, and enforcement support that is not yet fully available. This comparative perspective highlights that regulatory coherence is not only a matter of legal design but also of institutional readiness and the practical conditions needed to make such legislation effective.

2.7 Consolidated Legal and Institutional Gaps

- **Trust services and electronic signatures**: Although the Electronic Transactions Law recognizes the legal validity of electronic signatures and electronic records, the national trust services framework has not yet been activated. No supervisory authority has been designated, no TSPs have been licensed, and no national certification infrastructure has been established, limiting the use of electronic signatures in general civil, commercial, and public sector transactions.
- **E-commerce oversight capacity**: The e-commerce Decree assigns extensive regulatory responsibilities to the MoNE. While the Ministry's restructuring plan includes a dedicated e-

commerce unit, key implementation tools, such as the Electronic Commerce Register, digital supervision mechanisms, and structured complaint handling systems, remain under development and depend on the issuance of executive regulations.

- **Personal data protection**: Consumer data obligations under the e-commerce Decree remain narrow in scope in the absence of a comprehensive data protection law. Gaps persist in areas such as data subject rights, breach notification, cross-border data transfers, and enforcement mechanisms.
- **Cybersecurity regulation**: The current legal framework does not set out explicit cybersecurity obligations tailored to e-commerce platforms. Cybersecurity requirements are expected to be addressed through sectoral regulations or future policy instruments, resulting in uneven coverage.
- **Competition in digital markets**: Decree No. 11 of 2025 on Competition establishes a modern framework for prohibiting anticompetitive agreements, regulating abuse of dominance, and overseeing merger control. However, the law remains technology-neutral and does not include provisions specifically tailored to digital or platform-based markets. As a result, competition issues arising in e-commerce and digital payment services continue to be assessed using general competition law tools, which may not fully capture the specific dynamics of digital markets.
- **Regulatory coordination**: Effective implementation of the digital economy framework requires sustained coordination among multiple authorities, including the MoNE, the PMA, and the telecommunications regulator, particularly in areas of oversight, enforcement, and technical standards.

3. Institutional and Market Readiness for the Digital Economy

3.1 Regulatory and Institutional Developments

This section contextualizes the legal framework by examining how institutional priorities, market dynamics, and behavioral factors shape implementation and adoption in practice. Taken together, these developments explain why the payments sector has advanced faster than other components of the digital economy, while trust in broader digital transactions remains uneven. Based on consultations and meetings conducted with PMA, MoNE, and PCMA, this section presents an assessment of the electronic payment sector, financial inclusion efforts, and the challenges facing digital transformation in the financial ecosystem.

The foundation of digital financial transformation has been established through critical legislative and regulatory advancements. National Payment Decree No. 41 of 2022 serves as the cornerstone that enabled electronic payment services. This decree has been instrumental in organizing the sector, which now comprises six licensed electronic payment companies under PMA supervision. Significantly, the law has also reduced commission fees on electronic payments, making digital transactions more accessible and cost-effective for users.[37]

The National Switch Law represents another pivotal achievement in the regulatory landscape. This legislation enables seamless interoperability between banks and financial institutions, allowing individuals and businesses to conduct transactions such as cash withdrawals or transfers regardless of which bank they use. For example, a customer of the National Bank can utilize automated teller machines operated by Palestine Bank without restriction. This cross-institutional functionality has eliminated traditional barriers and created a more integrated financial ecosystem.[38]

The national strategy for financial inclusion, which commenced in 2018 and was originally set to conclude in 2025, has demonstrated measurable progress despite encountering numerous challenges. The plan has been developed and monitored through the National Committee for Financial Inclusion, which brings together representatives from all relevant governmental and regulatory bodies. Based on comprehensive assessments and ongoing challenges, a formal recommendation has been submitted to the Council of Ministers to extend the strategy's timeframe by an additional three years, contingent upon revision of the action plan.[39]

The regulatory approach to financial sector development follows a fundamental principle: legal and regulatory frameworks should be driven by market need rather than imposed in advance of demand. This philosophy recognizes that regulation alone does not create market activity or innovation. A clear illustration of this principle can be found in the investment fund sector, where a comprehensive regulatory framework for investment fund licensing has been established. Yet, no investment funds have been created under it. This demonstrates that regulatory permission alone is insufficient without genuine market demand and viable business models.[40]

The regulatory framework operates on the principle of allowing operations within defined boundaries rather than imposing rigid restrictions. Financial innovation is inherently broad and dynamic, and it cannot be entirely confined within a single, prescriptive legal framework. This approach provides flexibility for innovation while maintaining necessary oversight and control. It allows the sector to evolve in response to market needs and technological developments while ensuring consumer protection and systemic stability.

37 Anan Al-Samri (PMA), interview by author, October 28, 2025.
38 Ibid.
39 Bashar Abu Zarour (PCMA), interview by author, October 19, 2025.
40 Ibid.

A critical gap remains in the legal framework for cybersecurity and data protection. While efforts are ongoing to develop comprehensive legislation on both fronts, these laws have not yet been finalized or enacted. This absence poses significant challenges for the electronic payment sector, as robust data protection and cybersecurity frameworks are instrumental in building trust and ensuring the security of digital financial transactions. The lack of clear legal standards and requirements creates uncertainty for service providers and elevates risks for consumers.[41]

3.2 Inclusion and Access to Digital Financial Services

In 2022, a comprehensive assessment of financial inclusion was conducted, examining both demand and supply-side perspectives, with particular emphasis on Micro, Small, and Medium Enterprises (MSMEs). This assessment generated critical insights that informed subsequent policy decisions. Following the establishment of a unified definition for MSMEs, a significant milestone in itself, a steering committee was formed to guide sector development. The committee operates under the leadership of the Ministry of National Economy and includes representatives from the Palestinian Monetary Authority, the Palestine Capital Market Authority, and the Ministry of Finance.[42]

The financial inclusion strategy is structured around three fundamental pillars:[43]

First Pillar: Access to Financial Services
This pillar has achieved substantial progress. The access rate to financial services has risen to 62%, compared to 36% in 2016, representing nearly a doubling of access during this period. This progress demonstrates that the infrastructure and availability of financial services have expanded significantly, reaching a much broader segment of the population than previously possible.

Second Pillar: Usage of Financial Products and Services
Despite progress in access, this pillar remains a major challenge. The gap between availability and actual utilization of financial products indicates that access alone is insufficient. The core challenge lies in the affordability of financial products and their alignment with the needs of MSMEs and other target populations. There is a critical need for demand-oriented financial products that respond to genuine market requirements rather than simply providing generic services.

Third Pillar: Quality of Financial Products
This pillar addresses the need for financial products and services to meet appropriate standards and effectively serve their intended purposes. Quality encompasses not only the technical functionality of products but also their relevance, reliability, and suitability for different market segments.

A significant shift has occurred regarding the requirement to maintain traditional bank accounts. Initially, holding a bank account was a prerequisite for participating in the formal financial system. This requirement is no longer considered a major barrier to financial inclusion. The proliferation of e-wallets, E-Sadad, and other digital payment platforms has enabled many electronic transactions to be conducted without a traditional bank account. This development has substantially lowered the entry threshold for financial participation.[44]

3.3 Market Dynamics and Competition in Electronic Payments

The electronic payment sector in Palestine operates under the regulatory supervision of the PMA, with six licensed electronic wallet providers currently authorised to offer payment services. In parallel, centrally managed electronic billing and payment platforms operate within the national payments infrastructure. The coexistence of licensed payment service providers and central payment platforms

---

41 Interview with Mr. Anan Al-Samri, PMA, 28/10/2025.
42 Interview with Mr. Bashar Abu Zarour, PCMA, 19/10/2025.
43 Interview with Mr. Bashar Abu Zarour, PCMA, 19/10/2025.
44 Interview with Mr. Bashar Abu Zarour, PCMA, 19/10/2025.

reflects the current structure of the sector as regulated by the PMA. The practical interaction between these components, including their respective roles in facilitating payments and bill presentment, remains subject to ongoing regulatory oversight and further policy development.[45]

Licensing decisions in the electronic payment sector are closely linked to broader market-structure considerations, including the balance between the number of licensed providers and the overall level of demand for electronic payment services. Regulatory authorities therefore assess market capacity when considering the admission of additional electronic payment companies, to maintain sector stability and operational viability. The implications of this approach for market entry, innovation, and competitive dynamics depend on how demand for digital payments evolves and how the regulatory framework continues to develop.[46]

3.4 Cash Usage, Cash-On-Delivery, and Financial Culture

Beyond technical and regulatory issues, the sector faces fundamental challenges rooted in financial culture and levels of financial literacy. There is a recognized weakness in financial literacy across segments of the population, which affects the adoption and effective use of financial products and services. Many individuals lack the knowledge and confidence required to engage with electronic payment systems, digital wallets, and other financial technologies. This cultural barrier slows the pace of digital transformation and reduces the effectiveness of investments in digital payment infrastructure.[47]

Government services have not yet been fully digitized, which limits the potential for electronic payments to become the default mode of transaction across the economy. When government services continue to operate primarily through cash or traditional methods, this reinforces cash-based habits among the population and slows the transition to digital alternatives. Comprehensive digitization of government services would provide both a model and a practical incentive for the broader adoption of electronic payments.[48]

3.5 Tax Compliance, Delivery Services, and Informality Pressures

Nevertheless, while the technical requirement for bank accounts has been eliminated, other structural challenges persist. The transition from cash to electronic payments remains a significant structural hurdle. Cash and liquidity continue to circulate in ways that are difficult to control or monitor, and this largely unregulated cash economy competes with formal electronic payment systems. Encouraging broader adoption of electronic payments would enhance oversight, reduce transaction costs, and integrate a greater share of economic activity into the formal financial system.[49]

The rise of e-commerce has introduced significant challenges related to tax justice, which must be examined from two interrelated perspectives:[50]

- From the Perspective of Traditional Commerce: Traditional business owners increasingly perceive competition from e-commerce as a significant burden, negatively affecting their operations.
- From the Perspective of the State and its Fiscal Rights: There is a fundamental need to achieve tax justice and ensure that all commercial activities contribute equitably to public revenue.

Delivery companies play a crucial role in the e-commerce ecosystem, serving as the operational link between consumers and online stores. They directly handle interactions with both parties and are

45 Interview with Mr. Bashar Abu Zarour, PCMA, 19/10/2025.
46 Interview with Mr. Anan Al-Samri, PMA, 28/10/2025.
47 Interview with Mr. Anan Al-Samri, PMA, 28/10/2025.
48 Interview with Mr. Anan Al-Samri, PMA, 28/10/2025.
49 Interview with Mr. Anan Al-Samri, PMA, 28/10/2025.
50 Interview with Mr. Rashad Yousef, MoNE, 04/11/2025.

responsible for the physical movement of goods. Given their central position in the transaction chain, their role in regulatory and tax compliance is a key consideration.[51]

It is proposed that, for tax and regulatory purposes, any official document accompanying the goods, such as a receipt or a delivery note, should be considered sufficient proof of transaction. This approach would be preferable to requiring a traditional tax invoice for every transaction, as not all sellers, particularly small-scale or informal ones, are equipped to issue formal tax invoices. Recognizing alternative forms of documentation would streamline compliance process, reduce the burden on small merchants, and facilitate compliance without stifling the growth of e-commerce.[52]

3.6 National Digital Initiatives and Platforms

A strategic initiative led by MoNE is underway to establish a National Platform designed to centralize and formalize online interactions, shifting public engagement away from social media platforms toward a monitored and regulated environment. This platform aims to build trust among all parties by providing a secure and reliable ecosystem for dispute resolution and the organisation of complaints.[53]

This initiative is also linked to the promotion and encouragement of the Palestinian national domain, domain.ps. The goal is to encourage users and businesses to adopt the domain, thereby strengthening the national digital identity. However, concerns have been raised regarding the transition to mandatory use of domain.ps. To address these concerns, a phased approach is planned. The initial six months will focus on rectifying the current situation and addressing existing operational issues, followed by a gradual and managed transition to registration under domain.ps.[54]

The electronic payment sector and financial inclusion efforts have achieved substantial progress, particularly in establishing regulatory foundations and expanding access to formal financial services. The near-doubling of access rates from 36% to 62% represents a significant accomplishment. The development of interoperable payment systems, digital wallets, and unified platforms has contributed to a more inclusive and accessible financial ecosystem.

3.7 Role of Private Sector Bodies and Civil Society

The effectiveness of the legal framework governing e-commerce and electronic payments is shaped less by formal regulation than by the way compliance pathways are mediated in practice. In the Palestinian context, private sector representative bodies and civil society actors function as informal transmission mechanisms between regulation and market behaviour, particularly for MSMEs operating at the margins of formal economic activity.

Business membership organisations influence whether legal and regulatory requirements are perceived as feasible entry points into formalisation or as barriers to be avoided. Given that access to electronic payments is conditioned by tax registration, payment service onboarding, and platform requirements, these bodies often shape how businesses interpret compliance obligations and whether they engage with the formal digital economy or continue to rely on cash-based practices.

From the consumer side, civil society actors influence trust in electronic transactions by shaping perceptions of security, dispute resolution, and data protection. Persistent reliance on cash-on-delivery reflects not only economic considerations but also uncertainty regarding enforcement and access to redress mechanisms. In this sense, civil society engagement exposes a limitation of the current framework: legal recognition of digital transactions does not, on its own, produce behavioural change in the absence of credible trust mechanisms.

---

[51] Interview with Mr. Rashad Yousef, MoNE, 04/11/2025.
[52] Interview with Mr. Rashad Yousef, MoNE, 04/11/2025.
[53] Interview with Mr. Rashad Yousef, MoNE, 04/11/2025.
[54] Interview with Mr. Rashad Yousef, MoNE, 04/11/2025.

Together, these actors form an informal layer of governance that materially affects implementation outcomes. Where this layer is weak or fragmented, gaps between legal rules and market practice widen, limiting the effective reach of the digital economy framework.

4. Focus Group Findings

The focus group discussions provide a demand-side perspective that reflects the implementation gaps, coordination challenges, and institutional analysis set out in Sections 2 and 3. Rather than introducing new regulatory issues, the findings illustrate how existing legal and regulatory frameworks are experienced in practice by MSMEs operating within the Palestinian digital economy. In this sense, the discussions serve to test the practical adequacy of the current framework, particularly in relation to implementation, access to electronic payments, and the interaction between formal legal requirements and informal market practices. The two focus group discussions were conducted in Ramallah and Hebron with MSMEs, operating in various sectors of the digital economy. The findings reveal a consistent set of concerns across both groups, reflecting structural, legal, technical, and behavioural constraints that continue to limit the growth of digital commerce in Palestine.

4.1 Legal Uncertainty and Perceived Regulatory Burden

Participants expressed significant confusion regarding the legal obligations imposed by the recently enacted E-Commerce Decree-Law. MSMEs were particularly uncertain about the following:

- Registration requirements: whether home-based or informal sellers are required to register with the Ministry of National Economy.
- Penalties for non-compliance: which many participants perceive as excessively strict, including fines and potential imprisonment.
- Lack of differentiation between small informal sellers and larger enterprises, resulting in a perception that the law applies uniformly regardless of scale or capacity.

Many participants stressed that enforcement should be preceded by a period of awareness, guidance, and technical support. Unclear obligations, fear of penalties, and taxation discourage businesses from entering or expanding within the digital marketplace.

4.2 Limited Trust in Digital Payments and Barriers to International Trade

Participants highlighted constraints that hinder their ability to adopt digital payments or to reach international markets:

- Inaccessibility of global payment gateways for Palestinian businesses.
- High domestic transaction fees and limited trust in existing payment tools.
- Recognized need for a trusted Palestinian digital financial institution capable of facilitating cross-border transactions.

MSMEs emphasised that recent legal reforms were not matched by measures enabling international e-commerce participation.

4.3 Weak Infrastructure and High Operational Costs

Several MSMEs highlighted the high cost and technical complexity of establishing and maintaining online platforms. Concerns included:

- Expensive website development and maintenance.
- Lack of standardized digital tools or templates tailored to small businesses.
- Limited access to technical assistance necessary for onboarding into e-commerce.
- Perceived inadequacy of the digital infrastructure required to support a reliable online ecosystem.

Participants further explained that they expect the market to increasingly shift toward “cluster websites”, large online platforms that host numerous small sellers and provide shared services such as marketing, logistics, or payment facilitation. Many MSMEs anticipate that they will eventually need to join such platforms in order to participate effectively in digital commerce and reduce their individual technical and financial burdens.

However, they expressed concern that these arrangements typically lack formal guarantees, leaving sellers without clear protections regarding:

- Payment settlement.
- Platform fees and conditions.
- Dispute handling.
- Continuity of their presence on the platform.

Participants emphasized that they expect these cluster platforms to become more dominant and therefore, they require legal and regulatory protections that define the rights and obligations between merchants and platform operators. Without such safeguards, MSMEs fear becoming dependent on intermediaries who operate without transparent standards or oversight.

These combined obstacles push many businesses to rely on social media platforms or informal hosting arrangements, where neither merchants nor consumers benefit from clear legal protections or regulated service standards.

4.4 Market Dynamics, Competition, and Protection of Local Products

A participant expressed fears of potential market monopolization and unregulated competition, particularly from foreign digital platforms, especially Israeli ones, entering Palestinian markets without oversight. MSMEs called for:

- Stronger protection for local e-commerce applications and platforms.
- Regulatory measures to ensure fair competition.
- Policies that support domestic digital initiatives.

These concerns reflect a broader need for a market environment that supports local innovation and shields small enterprises from unregulated external competition.

4.5 Need for Standardized Templates and Practical Guidance

Participants emphasized the need for the Ministry of National Economy to provide standardized templates for key e-commerce documents, such as terms and conditions, return policies, privacy notices, and complaint procedures. MSMEs noted that many small or home-based sellers lack the capacity to draft these documents independently, and that having ready-to-use templates would reduce compliance burdens and support more consistent, transparent online practices.

4.6 Taxation Barriers, Clearance Limitations, and Constraints on Formalization

Participants, particularly in Hebron, raised substantial concerns regarding taxation procedures and the issuance of tax invoices, noting that these requirements become especially complicated when selling to Palestinians in the 1948 territories, who constitute a major portion of their customer base. Such transactions depend on the maqasa (tax-clearance) system, established under the Paris Protocol and administered by Israel, which controls the transfer of tax revenues to the Palestinian Authority.

MSMEs reported that, in practice, the Palestinian tax authorities allow only ten clearance invoices per year, a limitation that does not reflect the actual volume of cross-border sales conducted by online merchants. This restriction disrupts payment collection, creates delays, and complicates accounting processes for businesses whose livelihoods depend on frequent transactions with customers inside the 1948 territories.

Participants stressed that these constraints are not merely administrative but arise from a broader political and structural environment in which the tax-clearance mechanism is subject to Israeli control, delays, and deductions. As a result, many MSMEs feel that formal registration exposes them to a system they cannot reliably depend on, discouraging compliance and pushing some businesses to operate informally or through alternative channels outside the formal tax framework.

MSMEs emphasized that without more flexible and predictable mechanisms for handling clearance invoices, whether through increased quotas, alternative procedures, or tailored arrangements, they cannot fully benefit from the recently enacted e-commerce and digital payment reforms.

The focus groups reveal a digital-economy environment characterised by legal uncertainty, limited trust in payment systems, high operational and technical barriers, weak institutional support, and structural taxation constraints. These findings provide essential demand-side evidence for assessing the adequacy of the legal and institutional framework discussed in the subsequent section.

Overall, the focus group findings confirm that the principal constraints facing MSMEs are not the absence of legal recognition of e-commerce or electronic payments, but rather the way in which regulatory requirements are applied and accessed in practice. Concerns related to registration, taxation, access to payment services, and reliance on cash-based transactions reflect structural features of the regulatory environment identified earlier in the paper. These findings reinforce the importance of addressing implementation clarity, institutional coordination, and market incentives, rather than focusing solely on additional legislative expansion.

5. Adequacy Assessment of the Legal and Institutional Framework

5.1 Overall Adequacy of the Legislative Framework

The legislative developments introduced between 2022 and 2025 represent a significant step toward establishing a coherent framework for regulating e-commerce, electronic transactions, and digital payments in Palestine, aligned with international practices. The structure of the laws, particularly the E-Commerce Law, the National Payments Law, and the Electronic Transactions Law, shows clear legislative intent to organise the digital market, strengthen consumer rights, and create a predictable environment for electronic contracting. On paper, the framework is thoughtful and responsive to many of the challenges seen internationally.

However, after reviewing the laws in depth, speaking with the relevant institutions, and listening to MSMEs in Ramallah and Hebron, it becomes evident that the adequacy of the framework in practice is substantially weaker than its adequacy in design. The main gap is not conceptual; it is operational.

The Electronic Transactions Law establishes trust services, electronic signatures, and digital identity, but these mechanisms remain technically inactive. No formal steps have yet been taken to activate this framework at the national level. Without a functioning supervisory authority, certification infrastructure, or recognized trust service providers, the law cannot yet play the role it was designed for. In daily commercial life, electronic signatures and authenticated digital records remain unusable.

The E-Commerce Law is new and promising, but its regulatory ecosystem is still forming. Key elements require implementing regulations, templates, and clear procedures. MSMEs repeatedly expressed uncertainty about:

- Who must register,
- How registration will work in practice,
- What obligations apply to micro- and home-based sellers,
- What penalties will be enforced, and
- Whether the State intends to use the law primarily for compliance, taxation, or support.

Furthermore, the law does not differentiate between imported goods and locally produced goods, despite their entirely different cost structures, supply chains, and competitive pressures. MSMEs argued that applying uniform obligations to both categories places local producers at a structural disadvantage, especially in a market already saturated with cheaper foreign imports.

5.2 Institutional Adequacy

The PMA is the only body whose digital framework is fully active and functioning at scale. Instant payments, QR-code payment regulations, AML/KYC systems, E-SADAD, iBURAQ, and digital identity (ID+) are all operational and contributing to financial inclusion.

In contrast, the MoNE, which is responsible for enforcing the E-Commerce Law, has assumed a significantly expanded mandate that is still in the process of being operationalised. While the Ministry's institutional restructuring plan envisages the establishment of a dedicated e-commerce unit, key implementation elements, including the activation of the Electronic Commerce Register, market conduct supervision tools, digital consumer-protection mechanisms, and structured online complaint-handling systems, remain under development. These functions require specialised staffing, technical systems, and inter-agency coordination mechanisms that have not yet been fully established.

5.3 Adequacy Relative to the Economy's Readiness

The legal framework assumes:

- Trust between the public and the regulator,
- Adequate technical infrastructure,
- Affordable digital financial services,
- Accessible payment gateways,
- Clear tax procedures for cross-border commerce,
- Functioning dispute-resolution mechanisms.

However, the economy does not yet provide these conditions. MSMEs' experience with the tax clearance system (Maqasa**)** is a clear illustration: regardless of legislative quality, a business cannot operate formally when it can only issue "ten invoices a year" for its largest customer base. Similarly, no national e-commerce law can compensate for the inability to accept payments from abroad. This gap between legal intention and economic reality is the primary reason why adequacy remains partial.

Taken together, these observations indicate that while the legal and regulatory framework has advanced significantly, particularly in the payments sector under the leadership of the PMA, the broader environment is not yet fully equipped to support the smooth implementation of newer digital-economy laws. The frameworks governing electronic transactions and e-commerce are structurally sound and reflect a clear legislative direction, but they still require activation through implementing regulations, institutional capacity-building, and clear procedural guidance that responds to the realities faced by Palestinian MSMEs. The adequacy of the system, therefore, lies more in its potential than in its present effect: the foundation is strong, but the transition from legislative intent to everyday usability will depend on phased implementation, coordinated institutional roles, and policy measures that recognise the economic and operational constraints under which businesses operate.

6. Recommended Reforms

The findings of this paper show that the main obstacle to Palestine's digital economy is not the absence of legislation, but the difficulty of implementing and operationalising existing legislation. The following reforms reflect realistic steps that align with institutional capacity and the needs expressed by MSMEs.

1. Activate the Electronic Transactions Law

A supervisory authority for trust services should be formally designated, followed by the establishment of a national framework for electronic signatures, timestamps, and digital seals. Without these tools, electronic contracting will remain largely theoretical and limited in practical application.

2. Issue implementing regulations for the E-Commerce Law

MoNE should issue clear regulations that define registration categories, specify obligations according to business size, and provide standardised templates for terms and conditions, refund policies, privacy notices and complaint procedures. This would remove ambiguity and lower compliance burdens on small and home-based sellers.

3. Strengthen consumer and data protection measures

Until a comprehensive data protection law is adopted, interim rules should be issued to govern online data collection, retention, consent, and breach notification. These measures should be aligned with the Consumer Protection Law to increase trust in online transactions.

4. Address structural barriers that discourage formalisation

The current limitations of the tax clearance system, particularly the quota of invoices that MSMEs can issue for customers inside the 1948 territories, should be reviewed. Even modest administrative adjustments would ease compliance and reduce incentives to operate informally. A related concern raised by MSMEs concerns the tax treatment of digital advertising costs. In many regional jurisdictions, advertising and marketing expenditures, including payments to foreign digital platforms, are deductible business expenses. In Palestine, however, such costs are generally not deductible because invoices issued by platforms such as Meta do not meet the formal requirements of a tax-compliant invoice under Palestinian tax law and cannot be validated through the tax-clearing mechanisms established under the Paris Protocol. As a result, businesses bear substantial and unavoidable promotional costs without the ability to recognise them for tax purposes. Developing a mechanism to acknowledge, verify, or partially credit verified digital advertising expenditures, within existing tax and clearance constraints, would bring Palestinian practice closer to regional norms and alleviate a significant financial burden on e-commerce businesses.

5. Support market readiness

Legal reforms should be accompanied by practical measures such as awareness campaigns, structured onboarding support for MSMEs, and guidance on accessing international e-commerce markets. Aligning implementation with actual readiness of businesses will improve adoption.

6. Improve coordination and dispute resolution

MoNE, the PMA, and the Consumer Protection Council should develop a unified and accessible mechanism for handling digital complaints. This would provide clarity for both merchants and consumers and ensure consistent enforcement across institutions.

7. Support the development of e-payment gateways by online platforms to reduce reliance on cash-based transactions and increase transparency in online commercial activity.

8. Embed private-sector compliance in digital market practices

Private-sector digital service providers, e-commerce platforms, and payment companies should integrate consumer-protection and data-handling obligations directly into their operational models. This includes standardised disclosures, clear contractual terms and accessible complaint mechanisms. Embedding compliance at the service-design and onboarding stages, particularly for MSMEs, will help translate legal requirements into consistent market practice and strengthen trust in digital transactions.

9. Strengthen civil-society support for awareness and accountability

Civil-society organizations should move beyond project-based interventions toward sustained engagement in digital literacy, consumer awareness, and market monitoring. By identifying recurring implementation gaps, supporting users and MSMEs, and channelling evidence-based feedback to relevant authorities, civil society can reinforce accountability and improve the practical effectiveness of digital economy reforms.

Taken together, these reforms would help translate recent legislative progress into tangible improvements in the digital market, bridging the gap between legal intent and practical use and creating a more predictable, trusted environment for online commerce and payments.

References

1. Palestinian Authority. (2006, April 27). *Consumer Protection Law No. 21 of 2005* (Palestinian Gazette No. 63, p. 29). Retrieved from http://muqtafi.birzeit.edu/en/Legislation/GetLegFT.aspx?LegPath=2005&MID=15136
2. Palestinian Authority. (2018, May 3). *Decision by Decree No. 10 of 2018 on Cybercrime* (Special Issue No. 16 of the Palestinian Gazette, p. 8). [in Arabic]. Retrieved from جرائم_الكترونية_رقم_10_لسنة_2018.pdf
3. Palestinian Authority. (2018, July 31). *Decision by Decree No. 27 of 2018 amending Consumer Protection Law No. 21 of 2005* (Palestinian Gazette Special Issue 18, p. 40). [in Arabic]. Retrieved from https://maqam.najah.edu/legislation/230
4. Palestinian Authority. (2022, August 14). *Decree-Law No. 41 of 2022 regarding National Payments* (Palestinian Gazette No. 193, p. 66). [in Arabic]. Retrieved from قرار_بقانون_رقم_41لسنه2022بشأن_المدفوعات_الوطني__ppR6xk4.pdf
5. Palestinian Authority. (2024, 25 November). *Decision No. (17) of 2024 on Electronic Transactions and Trust Services*. *Palestinian Gazette*, 220, 4. [in Arabic]. Retrieved from قرار_بقانون_بشأن_المعاملات_الالكترونية.pdf
6. Palestinian Authority. (2025). *Draft Law on Electronic Commerce.* [in Arabic]. Retrieved from https://www.mne.gov.ps/ckfinder/userfiles/files/.pdf

Appendix

Interviews

- Mr. Anan Al-Samri, PMA
- Mr. Bashar Abu Zarour, PCMA
- Mr. Rashad Yousef, MoNE, Policy Manager
- Mr. Yousef Zaid, PalPay