Social Science and Humanities Journal
sshjournal.com
Volume 10 Issue 03 March 2026 Page No. 9916-9923
DOI: https://doi.org/10.18535/sshj.v10i03.2216
Received 04 March 2026 | Accepted 16 March 2026 | Published 20 March 2026

Legal Challenges and Regulatory Responses to Digital Finance and E-Commerce Fraud in Bangladesh.

Silma Subah Chowdhury Chowdhury[1]* | Fouzia Sultana Chowdhury[2]

12 Senior Lecturer, Department of Law, Port City International University, South Khulshi, Chittagong, Bangladesh; Assistant Professor, Department of Natural Science (History), Port City International University, South Khulshi, Chittagong, Bangladesh

*Corresponding author: Silma Subah Chowdhury Chowdhury

Abstract

This study analyses Bangladesh's legal framework for regulating fraud in digital finance and e-commerce amid the rapid expansion of mobile financial services and online marketplaces. It finds that existing laws and regulatory measures are fragmented, reactive, and insufficient to address emerging forms of digital fraud, including payment scams, identity theft, and unauthorized transactions. Using a doctrinal approach, the research identifies key regulatory gaps and proposes legal and institutional reforms to enhance fraud prevention, enforcement, and consumer protection while supporting sustainable digital economic growth.

Keywords: ***Digital finance, E-commerce fraud, digital payment.***

1. Introduction

Bangladesh is experiencing rapid digital transformation in its financial and commercial sectors, driven by the expansion of mobile financial services, digital payments and platform-based e-commerce. [1]. Unauthorized transactions, phishing, online scams, non-delivery of goods and misuse of personal data have become increasingly common, undermining consumer trust and market integrity. Bangladesh's legal response remains fragmented, with multiple laws and regulatory instruments providing only partial and uncoordinated protection. Existing frameworks were not designed for platform-based commerce or evolving fintech risks, resulting in regulatory gaps and inconsistencies. Against this backdrop, this study examines the need for a more coherent legal approach to regulating digital finance and e-commerce fraud in Bangladesh.

2. Research Method

The study adopts a qualitative approach in which content analysis was used to examine statutes, subsidiary legislation, regulatory circulars, and policy documents relevant to digital finance and e- commerce fraud. This approach enables a systematic assessment of legal principles, institutional mandates and enforcement mechanisms.

3. Nature and Typology of Digital Finance and E-commerce Fraud

Digital finance and e-commerce fraud in Bangladesh is characterized by adaptability, hybridity and huge scale. Rather than relying solely on sophisticated technical breaches, many fraudulent schemes exploit behavioral vulnerabilities, regulatory ambiguity and institutional weaknesses. In the digital finance sphere, common practices include phishing and vishing attacks impersonating banks or MFS providers, SIM swap fraud enabling account takeovers, fake customer support channels, and manipulation of networks.[2] These practices frequently rely on deception, trust exploitation and information asymmetry rather than advanced hacking techniques. E-commerce fraud presents a distinct but interconnected set of challenges. Fake online shops, advance-payment scams, non-delivery or delayed delivery of goods, delivery of counterfeit or inferior products, and abuse of refund mechanisms are widespread. Social media-based commerce is particularly susceptible due to anonymity, weak seller verification and absence of standardized dispute resolution mechanisms. In many cases, platforms act as

facilitators without assuming clear responsibility for vetting sellers or compensating victims. A defining feature of contemporary digital fraud is converged. Payment fraud often facilitates e-commerce scams, while marketplace fraud generates financial crimes that fall within the regulatory ambit of digital finance. Many fraudulent operations are transnational, involving offshore accounts, foreign hosting services or cross-border payment channels. These dynamics challenge traditional legal concepts of jurisdiction, evidence and liability, exposing the limitations of territorially bound and sector-specific legal frameworks.

4. Consumer Protection Principles Governing Digital Commerce

Regulatory Architecture of Digital Finance in Bangladesh: The regulatory architecture of digital finance in Bangladesh has evolved incrementally, shaped by a combination of financial inclusion objectives, monetary stability concerns and anti-money laundering imperatives. Rather than emerging from a unified legislative framework, digital finance regulation consists of a layered assemblage of statutes, regulations, circulars and supervisory guidelines issued overtime. This architecture reflects a sectoral approach in which financial regulation, consumer protection and cyber governance operate in parallel, often without formal coordination. At the core of this architecture lies the central bank's supervisory authority over payment systems, mobile financial services and non-bank financial institutions. Regulatory instruments typically emphasize licensing, operational safeguards, transaction limits and compliance reporting[3]. While these measures have contributed to system stability and rapid market expansion, they are less attuned to consumer facing risks such as fraud, misrepresentation and dispute resolution. As a result, the regulatory architecture prioritizes imitational soundness over transactional fairness, leaving significant gaps in the governance of digital market conduct. The absence of a comprehensive digital finance statute further complicates regulatory coherence. Legal authority is dispersed across general banking laws, financial regulations and technology-related statutes, creating ambiguity regarding jurisdiction, enforcement responsibility and regulatory hierarchy. This fragmentation becomes particularly problematic when digital finance intersects with e-commerce, as transactions simultaneously implicate financial regulation, consumer law and platform governance norms.

Mobile Financial Services (MFS) and Agent Banking Framework: Mobile financial services (MFS) constitute the most prominent and widely utilized segment of Bangladesh's digital finance ecosystem. These platforms facilitate deposits, withdrawals, fund transfers, merchant payments, and utility bill payments through mobile devices and agent networks. The regulatory framework governing MFS prioritizes operational resilience, liquidity management, and anti-money laundering compliance, reflecting broader concerns regarding systemic stability and financial integrity. Agent banking operates alongside MFS as a hybrid model that extends conventional banking services through authorized agents. Although agent banking is subject to stronger institutional oversight, both systems depend heavily on intermediaries who engage directly with consumers. These agents perform essential functions, including customer onboarding, transaction processing, and dispute resolution, yet supervision at the point of service delivery often remains limited[4]. From a fraud regulation perspective, the extensive reliance on agent networks creates structural vulnerabilities. Insufficient monitoring, inadequate training, and misaligned incentives may enable deceptive practices, unauthorized transactions, and exploitation of consumer trust. Regulatory guidelines typically conceptualize agents as operational extensions of licensed institutions rather than as independent risk nodes requiring tailored governance mechanisms. This regulatory approach weakens preventive fraud controls and shifts disproportionate responsibility onto consumers to identify and report misconduct.

Digital Wallets, Payment Service Providers and Gateways: Digital wallets, payment service providers, and payment gateways form the infrastructural backbone linking digital finance with e-commerce. These entities facilitate fund transfers among consumers, merchants, and online platforms, operating as intermediaries that process, authenticate, and settle transactions in real time. Their regulatory treatment generally adopts a functional approach, concentrating on payment facilitation rather than the broader commercial environment in which transactions occur. Payment service providers are typically subject to licensing requirements, technical compliance standards, and transaction monitoring obligations. However, their consumer-facing responsibilities are often narrowly defined, prioritizing system reliability and data security over explicit fraud liability or compensation frameworks[5]. Payment gateways embedded within e-commerce platforms further complicate accountability, as they operate at the intersection of financial regulation and commercial law. This multi-layered payment architecture diffuses responsibility across several actors, complicating the allocation of liability in cases of fraud. Consumers frequently engage simultaneously with merchants, digital platforms, and payment intermediaries, each governed by distinct regulatory regimes. The absence of clearly defined rules delineating responsibility among these actors weakens deterrence mechanisms and undermines consumer confidence, particularly where fraudulent transactions involve multiple intermediaries.

Structure and Regulation of E-commerce Platforms and Market places: The e-commerce sector in Bangladesh comprises a heterogeneous range of platforms, spanning structured online marketplaces and informal social media-based commerce. Structured marketplaces typically offer integrated services, including product listings, payment facilitation, logistics coordination, and customer support. By contrast, social media commerce operates with minimal institutional structure, relying primarily on direct communication and informal arrangements between buyers and sellers. Regulatory oversight of e-commerce has largely evolved in a reactive manner,

responding to consumer complaints and market disruptions rather than through proactive, systematic governance. Regulatory interventions frequently take the form of guidelines or policy directives instead of binding statutory mandates. While such measures address registration requirements, disclosure standards, and baseline consumer protections, they provide limited clarity regarding platform liability for fraudulent conduct by third-party sellers. The platform-centric architecture of e-commerce raises fundamental issues of responsibility and control [6]. Platforms curate digital marketplaces, shape transaction flows, and derive economic benefit from user engagement. Nevertheless, prevailing regulatory frameworks often conceptualize them as passive intermediaries rather than as market organizers exercising structural influence. This conceptual misalignment enables platforms to externalize fraud-related risks onto consumers while retaining substantial control over market design, data governance, and transactional infrastructure.

Role of Bangladesh Bank, BTRC and Other Regulatory Bodies: Digital finance and e-commerce in Bangladesh are governed by multiple regulators with overlapping mandates. The central bank supervises payment systems and mobile financial services, emphasizing stability, compliance, and risk management. Telecommunications authorities regulate the digital infrastructure underlying mobile transactions, while consumer protection agencies address unfair trade practices. Law enforcement bodies handle the criminal dimensions of digital fraud [7]. Despite this multiplicity, coordination remains weak and jurisdictional boundaries are often unclear. A single fraudulent transaction may trigger financial, telecommunications, and consumer protection concerns, yet no authority assumes comprehensive responsibility. This institutional fragmentation constrains enforcement capacity. Regulators operate within narrowly defined mandates, limiting their ability to address cross-sectoral risks. The resulting siloed framework weakens fraud prevention and hampers the development of integrated regulatory responses suited to digital markets.

Emerging Trends and Systemic Vulnerabilities: Bangladesh's digital finance and e-commerce ecosystem is evolving rapidly, driven by technological innovation, market expansion, and shifting consumer behavior. Emerging trends include app-based service delivery, digital credit integration, cross-border payment expansion, and data-driven decision-making. While these developments improve efficiency and financial inclusion, they also generate new risk vectors. Systemic vulnerabilities stem from regulatory lag, which permits novel business models to operate in legal gray zones, and uneven enforcement that enables regulatory arbitrage [8]. High consumer trust, coupled with limited digital literacy, heightens exposure to deception. Dependence on mobile networks and third-party service providers further increases susceptibility to fraud and operational disruptions. These risks are structural rather than incidental. They reflect broader governance choices concerning market liberalization, regulatory prioritization, and institutional coordination. A systemic perspective is therefore essential to evaluate the adequacy of existing legal frameworks and to design reforms that address fraud as a market-wide governance challenge rather than as isolated incidents.

5. Forms and Dynamics of Digital Finance and Ecommerce Fraud in Bangladesh

This section examines the substantive patterns and operational dynamics of digital finance and e-commerce fraud in Bangladesh. It categorizes the principal forms of fraud that have emerged within the country's digital economy and analyzes the methods through which such frauds are carried out. It also assesses the broader consequences of digital fraud, highlighting its impact on individual consumers, market integrity, financial stability, and public trust in digital systems. By demonstrating the scale and complexity of these practices, this analysis underscores the inadequacy of fragmented and reactive regulatory responses.

Payment Fraud and Unauthorized Transactions: Payment fraud is a major economic threat in Bangladesh, primarily targeting mobile financial services and digital wallets. Fraudsters often use account takeovers, SIM swaps, or agent collusion to initiate unauthorized, irreversible transfers that are difficult to recover. Current regulations focus on system security but lack clear frameworks for liability and victim compensation. Legally, a major gap exists: while a transaction may be "technically" authorized through a password or PIN, it often lacks genuine consent if induced by deception. This creates a significant barrier for consumers seeking redress in an increasingly complex digital ecosystem [9].

Fake Online Shops and Marketplace Manipulation: Fake online shops and marketplace manipulation are major threats to e-commerce, especially on social media. Fraudsters use fake profiles and artificial demand like fake reviews to lure consumers into making advance payments for goods that are never delivered. Because these sellers can easily hide behind anonymity [10], they often vanish and reappear under new identities with minimal risk. A significant regulatory gap persists because current laws struggle with seller verification and platform accountability. While platforms benefit from high transaction volumes, they often lack the legal obligation to proactively police these scams. This leaves consumers vulnerable, as enforcement is frequently blocked by jurisdictional issues and the difficulty of proving fraud in informal digital spaces.

Non-Delivery, Partial-Delivery and Refund Scams: Non-delivery and refund scams occur when sellers fail to provide goods after payment or deliver items that are materially different from what was advertised. These schemes are often worsened by refund scams, where sellers or platforms use opaque procedures and indefinite delays to avoid returning money. This effectively denies consumers any functional remedy once a transaction goes wrong. Current legal and platform-based protections are often inadequate because they rely on traditional contract law, which assumes both parties are easily identifiable[11]. In the anonymous world of social media commerce, these assumptions fail. Without standardized,

binding dispute resolution mechanisms, enforcement remains discretionary, leaving the burden of loss and the struggle for redress entirely on the consumer.

Identity Theft, Phishing and Social Engineering: Identity theft and social engineering in digital finance are scams that target human psychology rather than technical flaws. Through phishing, vishing, and fake support channels, fraudsters trick users into revealing credentials by impersonating trusted entities like banks or mobile financial service providers. Once an account is compromised, it is often drained or used to facilitate further criminal activity. Current regulations struggle to keep pace because they focus on system security rather than human-centric deception. While laws criminalize data misuse, there is a "regulatory asymmetry": platforms are optimized for speed and convenience, yet the legal burden of protection rests almost entirely on the consumer. This gap leaves users vulnerable in environments where split-second decisions are encouraged over careful deliberation.

Cross-Border and Transnational Fraud Challenges: Transnational digital fraud is increasingly borderless, with criminals using foreign-hosted platforms, offshore accounts, and international payment channels to evade local laws. Even when a victim and a transaction are domestic, the underlying data or financial intermediaries often cross borders, stretching traditional, territory-based legal frameworks to their breaking point. These jurisdictional hurdles make investigation and prosecution extremely difficult. Regulatory authorities often lack the mandate or institutional capacity for international cooperation, leading to low recovery rates. Furthermore, fraudsters engage in regulatory arbitrage, deliberately operating from regions with weaker data protection or enforcement standards to minimize their risk of sanction.

Impact of Fraud on Consumers, Financial Stability and DigitalTrust: Digital fraud causes damage far beyond individual financial loss; it erodes the foundational trust necessary for a digital economy to function. For consumers--especially low-income or first-time users--fraud creates psychological stress and discourages the adoption of modern financial tools. When users fear every transaction, the convenience and scalability of digital platforms are lost. At a systemic level, high fraud rates threaten market integrity and financial stability. It forces legitimate businesses to face higher operational costs and stricter compliance, which can stifle innovation and favor unscrupulous actors who ignore the rules. Ultimately, because trust is the "currency" of the digital age, persistent fraud diminishes the social and economic benefits of technology. This underscores the urgent need for a preventive, consumer-centric regulatory framework that prioritizes safety over simple transaction speed.

6. Existing Legal and Regulatory Framework in Bangladesh

This section of the research critically examines the existing legal and regulatory framework governing digital finance and e-commerce fraud in Bangladesh. Rather than providing a purely descriptive account of statutory provisions, this researcher evaluates the scope, applicability and limitations of key laws and regulatory instruments in responding to technologically mediated fraud. By analyzing criminal law, consumer protection legislation, contract law, financial regulation and sector-specific directives, the chapter demonstrates how the current framework remains fragmented, reactive and inadequately aligned with the structural realities of the digital economy.

Digital Security Act 2018:Scope and Enforcement Challenges: The Digital Security Act (DSA) 2018 [12] is Bangladeshi's primary legal tool for tackling cyber offences, including unauthorized access and identity theft. However, its criminal-law focus emphasizes punishment and prosecution rather than practical consumer protection. While it provides a formal basis for addressing fraud, its design is better suited for direct technical hacks than for the complex, human-centric deception found in modern e-commerce.

Consumer Rights Protection Act 2009and E-commerce Transactions: The Consumer Rights Protection Act (CRPA) 2009 is Bangladesh's primary shield against unfair trade practices, misrepresentation, and defective goods. While its principles apply to e-commerce, the Act was designed for a **pre-digital era**, leaving it ill-equipped to handle the complexities of online marketplaces and digital payment systems. e.g. Structural Mismatches: **i) p**latformanonymity: The Act struggles with digital marketplaces where sellers are anonymous or located across borders, making traditional administrative complaints difficult to enforce; **ii) Liability Gaps:** There is no clear legal allocation of responsibility between the seller, the platform, and the payment gateway. This forces consumers to chase individual sellers even when the platform facilitated the transaction; **iii) Limited Remedies**: The enforcement model relies heavily on criminal sanctions and administrative fines rather than providing clear civil remedies or collective redress for defrauded groups.

Contract Act 1872 and Digital Contracts: It provides the foundational principles of offer, acceptance, and consent for all agreements in Bangladesh, including those made online. However, this 19th-century law struggles to regulate the fast-paced reality of digital contracting, where agreements and automated processes often replace meaningful negotiation.

Theoretical vs. Digital Reality: i)Consent Gap: The Act assumes equal bargaining power, but digital consumers rarely read or negotiate standardized terms, leading to asymmetrical dynamics where platforms hold all the power. **ii) Anonymity& Enforcement**: Traditional contract law relies on identifying specific parties. In digital fraud, sellers are often anonymous or offshore, making it nearly impossible to establish a breach or enforce a judgment; **iii) Impractical Remedies**: The time and cost of pursuing a standard breach-of-contract case far outweigh the value of most e-commerce transactions, rendering the Act a weak corrective tool for everyday fraud.

Penal Code 1860 and Traditional Fraud Offences: The Penal Code 1860 remains the bedrock for criminalizing fraud and cheating in Bangladesh. While its definitions are broad enough to cover digital deception, the Code was built for direct,

person-to-person crimes, making it difficult to apply to the layered, automated nature of modern e-commerce.

ICT Act Provisions Relevant to Digital Transactions: The Information and Communication Technology (ICT) Act 2006 [13] was Bangladesh's first major step into regulating digital misconduct, focusing on unauthorized access and the legal validity of electronic records. While it laid the groundwork for digital law, its scope is strictly technological rather than consumer-oriented, making it an outdated tool for modern e-commerce disputes. The key limitations of this act are e.g. **Limitations in the Modern Market: i) Technical Bias**: The Act targets and technical violations but ignores deceptive market conduct, platform liability, and consumer redress**.ii) Legislative Overlap**: As newer laws like the Digital Security Act (and now the Cyber Security Act) emerged, the ICT Act's role has become blurred, leading to interpretive uncertainty in court. **iii) Missing Intermediaries:** It lacks provisions to hold platforms or payment gateways accountable, focusing only on the individual behind a computer.

Money Laundering Prevention Act 2012 and Financial Crime Control: Itserves as Bangladesh's primary tool for detecting illicit fund flows and terrorist financing. While digital finance platforms must comply with its reporting standards, the Act is a systemic shield, not a consumer one. It focuses on institutional integrity rather than recovering money for individual fraud victims. However, this act also has some key limitations those are e.g. i) **Systemic vs. Individual:** The Act targets financial risks. It is designed to catch large- scale laundering, not to help a single user resolve an e-commerce scam. ii) **Small AmountGap:** Many digital fraud cases involve small individual sums that may fall below the threshold for intense MLPA scrutiny, even though their cumulative impact on public trust is massive. iii) **Compliance vs. Prevention**: Its framework prioritizes reporting and auditing by banks and platforms rather than proactive consumer safeguards or "know your customer" (KYC) improvements specifically aimed at fraud prevention.

Bangladesh Bank Circulars and Regulatory Directives on DigitalPayments: Bangladesh Bank Circulars are the primary tool for governing mobile financial services (MFS) and payment providers. While they are highly effective at ensuring systemic stability--setting licensing rules, transaction limits, and security standards--they are primarily "prudential" meaning they focus on the health of the financial system rather than the rights of the individual user [14]. The key limitations of this act are e.g. **i) Prudential Bias:** The directives prioritize risk management and liquidity over consumer redressor platform accountability**. ii) Shift of Responsibility**: Fraud prevention often relies on user awareness, effectively placing the legal and financial burden on the consumer to avoid being tricked. **iii) Legal Uncertainty**: Because these are circulars rather than primary legislation (laws passed by Parliament), they often lack binding rules for liability allocation or mandatory victim compensation**.iv) TheGrey Area**: Without a formal law, it is difficult to enforce dispute resolution when complex fraud involves multiple banks or third-party apps.

Overlaps, Gaps and Inconsistencies in the Legal Framework: The legal landscape in Bangladesh is currently a fragmented framework where multiple laws are address aspects of digital fraud, yet none provide a comprehensive, integrated response aligned with the convergence of digital finance and E-commerce. Overlaps arises where criminal, consumer, and financial laws apply simultaneously without clear co-ordination. This creates "legislative clutter" where regulators and victims are often unsure which law takes precedence, leading to institutional confusion and inconsistent enforcement. critical vulnerabilities [15]. There are some key limitations of this act. e.g. **i) The Responsibility Gap:** There is no clear legal consensus on platform liability or the responsibility of intermediaries like payment gateways when a scam occurs. **ii) Reactive vs. Proactive**: The current approach is largely reactive, focusing on punishing criminals after the fact rather than building a preventive, consumer-centric ecosystem. **iii) Lack of Integration**: While technology has converged finance and e-commerce now live on the same apps, the laws remain isolated in their original

7. Enforcement Mechanisms and Practical Challenges

This section of this research examines how the existing legal and regulatory framework governing digital finance and e-commerce fraud in Bangladesh operates in practice. By analyzing the roles of law enforcement agencies, regulatory bodies and courts, the researcher highlights the structural, procedural and capacity-related challenges that undermine effective prevention, investigation, adjudication and victim redress in digital fraud cases.

Role of Law Enforcement Agencies in Digital Fraud Investigation: Law enforcement agencies play a central role in responding to digital finance and e-commerce fraud, primarily through investigation, arrest and prosecution under criminal statutes. Digital fraud complaints are generally treated as cybercrime or financial crime matters, falling within the jurisdiction of police units tasked with handling technology-related offences. These agencies are responsible for receiving complaints, securing digital evidence and initiating criminal proceedings. In practice, law enforcement responses are largely reactive and complaint-driven. Investigations are typically initiated only after significant harm has occurred, with limited emphasis on preventive intelligence gathering or market-level risk analysis. The focus on individual perpetrators rather than systemic enablers reflects the criminal law orientation of enforcement, which is ill-equipped to address platform-mediated and structurally facilitated fraud. Moreover, law enforcement agencies often operate without specialized regulatory insight into digital finance and e-commerce systems. This limits their ability to understand complex transaction flows, intermediary roles and platform architectures. As a result, investigations may be narrowly framed, overlooking contributory negligence or governance failures by platforms and intermediaries that enable fraudulent activity.

Cyber Crime Units and Technical Capacity Constraints: Specialized cybercrime units have been established to address technology-enabledoffences, including digital fraud. These units are tasked with digital forensics, dataanalysis and coordination with service providers to trace transactions and identifyoffenders. Their existence reflects institutional recognition of the distinct challengesposed by digital crime.Despite this specialization, significant capacity constraints persist. Limited technicalexpertise, outdated forensic tools and insufficient training hinder effectiveinvestigation. Rapid technological change further exacerbates these challenges, asfraud techniques evolve faster than institutional learning and resource allocation [16].Cybercrime units may also be overstretched, handling a wide range of offences beyond digital finance and e-commerce fraud. Capacity constraints are compounded by dependence on cooperation from private entities such as mobile operators, payment service providers and platforms. Delays in data access, inconsistent record-keeping and lack of standardized information-sharing protocols impede timely investigation [17]. These structural limitations reduce detection rates and weaken deterrence, allowing fraud to proliferate with relatively low enforcement risk.

Jurisdictional and Evidentiary Challenges in Digital Fraud Cases: Jurisdictional complexity represents one of the most significant barriers to effective digital fraud enforcement. Digital transactions often transcend territorial boundaries, involving offshore servers, foreign platforms or cross-border payment channels. Determining the appropriate forum, applicable law and investigative authority becomes particularly challenging in such cases. Evidentiary issues further complicate enforcement. Digital evidence is often volatile, distributed across multiple systems and controlled by private intermediaries**.** Establishing authenticity, chain of custody and admissibility requires technical expertise and procedural safeguards that may be inconsistently applied. Traditional evidentiary standards, designed for physical documents and tangible property, are often ill-suited to electronic records and automated processes. These challenges disproportionately affect victims, who may lack the resources or knowledge to navigate complex legal procedures. Delays and uncertainty injurisdictional and evidentiary matters undermine confidence in enforcement institutions and discourage reporting, contributing to under-detection of digital fraud [18].

Inter-Agency Coordination and Information Sharing: Effective regulation of digital fraud requires coordination among multiple agencies,including law enforcement, financial regulators, telecommunications authorities andconsumer protection bodies. Each institution possesses partial information andlimited jurisdiction, making cooperation essential for comprehensive enforcement.In practice, inter-agency coordination remains weak and largely ad hoc. Institutionalsilos, overlapping mandates and absence of formal information-sharing frameworks hinder collaboration. Data relevant to fraud detection and investigation is often fragmented across agencies, limiting the ability to identify patterns or systemic risks. The lack of coordinated governance also affects regulatory accountability [19]. No single authority assumes overarching responsibility for digital fraud control, leading to diffusion of responsibility and inconsistent enforcement outcomes. Strength eninginter-agency coordination is therefore critical for transitioning from reactiveen forcement to proactive, risk-based regulation [20].

Victim Redress, Compensation and Dispute Resolution Gaps: Victim redress constitutes one of the most neglected aspects of digital fraud regulation in Bangladesh. Existing enforcement mechanisms prioritize criminalprosecution over compensation and restitution. Victims are often required to navigate complex administrative and judicial processes to recover losses, with uncertain outcomes. Alternative dispute resolution mechanisms in digital finance and e-commerce are underdeveloped. Platform-based complaint systems may lack transparency, independence or binding authority. Regulatory complaint mechanisms are often slow and inaccessible, particularly for vulnerable consumers with limited digital literacy. The absence of clear liability allocation among platforms, payment providers and sellers' further complicate redress. Victims may face a "responsibility vacuum" in which each actor denies liability, leaving consumers without effective remedies. This systemic failure undermines consumer trust and weakens the legitimacy of digital markets [21].

Evaluation of Judicial Responses and Case Law Trends: Judicial responses to digital finance and e-commerce fraud in Bangladesh remain limited and uneven. Reported case law is sparse, reflecting low levels of litigation, reliance on informal resolution and procedural barriers. Where cases do reach the courts, judicial reasoning often applies traditional legal doctrines without fullyengaging with the technological and structural dimensions of digital fraud. Courts tend to focus on individual culpability rather than systemic governance issues. Questions of platform liability, intermediary responsibility and regulatory negligenceare rarely addressed in depth. This narrow judicial approach limits the development of jurisprudence capable of guiding regulators, platforms and consumers in digital markets. Nevertheless, emerging judicial engagement with digital evidence and electronictransactions indicates gradual adaptation. Over time, consistent and informed judicialinterpretation could play a crucial role in shaping regulatory expectations and accountability standards. However, without complementary legislative reform and institutional capacity building, judicial intervention alone is unlikely to resolve the structural challenges of digital fraud enforcement.

8. Discussion

This portion of research set of reform proposals and policy recommendations aimed at addressing the structural and normative deficiencies identified in the preceding. Researcher is drawing his attention on the conceptual framework, empirical patterns of fraud, enforcement challenges and comparative insights, this portion of research urges for a coherent, future-oriented regulatory approach to digital finance and e-commerce fraud in Bangladesh. The proposals seek to balance innovation and market growth with legal control, trust

and accountability.

Need for a Unified Digital Fraud Regulatory Framework:A central weakness of the existing legal regime is its fragmented and sector-specific nature. Digital fraud regulation in Bangladesh is dispersed across criminal law, consumer protection statutes, financial regulations and technology-related legislation, none of which provide a comprehensive response to the convergence of digital finance and e-commerce. This fragmentation creates regulatory blind spots, weakens enforcement and places disproportionate responsibility on consumers. A unified digital fraud regulatory framework would consolidate core principles, define institutional responsibilities and establish coherent standards applicable across platforms, payment systems and marketplaces [22]. Such a framework should integrate preventive obligations, liability allocation and redress mechanisms rather than relying solely on ex post criminal sanctions. Importantly, unification does not require the replacement of existing laws but their harmonization through an overarching statute or coordinated regulatory architecture that reflects the realities of digital transactions.

Strengthening Platform Liability and Due Diligence Obligations: Reform must recalibrate the legal position of platforms from passive intermediaries to accountable market organizers. Platforms exercise significant control over transaction environments through design choices, data management and rule-setting functions. This capacity for control justifies corresponding legal responsibility for fraud prevention and consumer protection. Policy reforms should impose explicit due diligence obligations on platform, including robust seller verification, transaction monitoring and timely response to fraud complaints. Conditional liability models can balance accountability with innovation, granting platforms limited liability protections only where they demonstrate compliance with prescribed governance standards. Such an approach incentivizes proactive risk management while avoiding excessive regulatory burdens that could stifle market entry. Strengthening platform liability also requires clarity in law [23]. Clear statutory provisions allocating responsibility among platforms, sellers and payment intermediaries would reduce ambiguity, enhance deterrence and improve consumer confidence in digital marketplaces.

Risk-Based Fintech Regulation and Supervisory Innovation Traditional rule-based regulation is ill-suited to the pace and complexity of digital innovation. A shift toward risk-based fintech regulation would allow regulators to prioritize high-risk activities, adapt to emerging threats and allocate resources more effectively. Risk assessment should consider transaction volume, consumer exposure, technological complexity and cross-border elements. Supervisory innovation plays a critical role in this approach. Tools such as regulatory sandboxes, data-driven supervision and collaborative regulatory forums enable regulators to engage proactively with fintech firms and platforms [24]. These mechanisms facilitate learning, experimentation and early identification of fraud risks without imposing blanket restrictions. Embedding risk-based regulation within the broader supervisory framework would enhance regulatory agility and align oversight with actual market dynamics. Such reforms require institutional capacity building and legal mandates that support flexible, adaptive governance.

Enhancing Cyber-Investigation Capacity and InstitutionalCoordination: Effective fraud regulation depends on strong investigative and enforcement capacity. Enhancing cyber-investigation capabilities requires investment in technical expertise, forensic tools and continuous training for law enforcement agencies. Specialized units should be adequately resourced and empowered to handle complex digital transactions and cross-border cases. Institutional coordination is equally critical. Formal mechanisms for information sharing among financial regulators, telecommunications authorities, consumer protection agencies and law enforcement bodies should be established. Coordinated governance reduces duplication, clarifies accountability and enables systemic risk analysis. Policy reforms should also promote public-private cooperation [25]. Platforms and payment providers possess valuable data and technical knowledge that can support fraud detection and prevention when appropriately regulated. Structured collaboration can enhance enforcement effectiveness while safeguarding privacy and due process.

Specialized Redress and Adjudication Mechanisms for Digital Fraud: Victim redress must be elevated from a peripheral concern to a core regulatory objective. Existing mechanisms are slow, fragmented and inaccessible, particularly for vulnerable consumers. Establishing specialized redress and adjudication mechanisms tailored to digital fraud would significantly enhance consumer protection. Such mechanisms could include dedicated digital dispute resolution bodies, ombudsman schemes or fast-track tribunals with technical expertise [26]. Simplified procedures, time-bound resolution and binding outcomes would improve accessibility and effectiveness. Importantly, redress mechanisms should incorporate clear liability rules, enabling consumers to obtain compensation without navigating complex institutional hierarchies. Integrating redress mechanisms within the regulatory framework reinforces trust and complements preventive regulation by ensuring accountability when harm occurs.

Strengthening Data Protection and Consumer Trust: Data protection is a foundational element of digital fraud regulation. Weak data governance exacerbates identity theft, phishing and social engineering scams, undermining consumer trust. Strengthening data protection requires comprehensive legal standards governing data collection, use, storage and sharing across digital finance and e-commerce platforms. Reforms should emphasize transparency, informed consent and security safeguards, alongside effective enforcement mechanisms. Breach notification obligations and meaningful penalties for non-compliance enhance accountability and deterrence. Aligning data protection with consumer protection and financial regulation creates a cohesive governance environment that supports trust and market legitimacy. Consumer trust is not merely an outcome but a regulatory objective. By embedding trust-enhancing measures into legal design, regulators can foster sustainable digital market growth.

Roadmap for Legal and Regulatory Reform in Bangladesh: A pragmatic roadmap for reform should prioritize sequencing, feasibility and institutional capacity. Short-term measures may include enhanced regulatory coordination, updated guidelines and capacity building for enforcement agencies. Medium-term reforms could focus on statutory amendments clarifying platform liability, consumer redress and data protection obligations. Long-term reform requires the development of an integrated digital fraud regulatory framework that reflects convergence, risk and platform accountability. This process should involve stakeholder consultation, comparative benchmarking and iterative evaluation to ensure responsiveness to technological change [27]. By adopting a phased and holistic approach, Bangladesh can transition from fragmented and reactive regulation toward a coherent system that balances innovation, inclusion and protection. Such reform is essential for building a resilient digital economy grounded in trust, fairness and accountability.

This research has examined the regulation of digital finance and e-commerce fraud in Bangladesh against the backdrop of rapid technological transformation and market expansion. The central argument advanced throughout the study is that digital fraud in Bangladesh is not merely a problem of individual criminal conduct but a manifestation of deeper structural, regulatory and governance failures within an increasingly convergent digital economy. Traditional, sector-specific and reactive legal approaches have proven insufficient to address fraud risks embedded in platform-based commerce, intermediary-driven payment systems and data-intensive market practices. Payment fraud, marketplace manipulation, identity-based deception and cross-border schemes illustrate the inadequacy of legal frameworks that rely primarily on ex post criminal sanctions and individual liability. These dynamics underscore the need for preventive, system-oriented regulation that addresses market design and intermediary incentives. Enforcement challenges further compound these doctrinal weaknesses, as law enforcement agencies and regulators face jurisdictional complexity, evidentiary constraints, limited technical capacity and fragmented institutional mandates. By aligning legal frameworks with the structural realities of digital markets, Bangladesh can protect consumers, enhance market integrity and sustain trust in its digital economy. The findings of this research contribute to legal scholarship by offering an integrated analytical framework and to policy discourse by outlining a practical roadmap for regulatory reform. As digital technologies continue to evolve, future research should further explore empirical dimensions of fraud, the role of emerging technologies in regulation and the long- term impact of platform governance on market fairness and inclusion.

References

1. M. o. Commerce, "National E-commerce Policy: Goverment of Bangladesh," Dhaka, 2020. 10.3329/jbt.v10i1.26905
2. M. Hossain, "Patterns of Digital Payment Fraud in Bangladesh," Asian Journal of Criminology, vol. 16, no. 3, pp. 189-210, 2021. 10.4324/9780429320118-30
3. C. C. A. F. (CAF), "Cyber Crime trend in Bangladesh," Cyber Crime Awarness Foundation, Dhaka, 2022. 10.1093/oso/9780198723905.003.0004
4. R. a. K. N. Islam, "E-Commerce Fraud and Consumer Vulnerability," Dhaka University Law Review , vol. 15, no. 1, pp. 55-84, 2020. 10.2307/3311528
5. The Digital Security Act, 2018. 10.4324/9781351171564-2
6. 2. Information and Communication Technology Act. 10.1093/acrefore/9780190228613.013.895
7. B. Bank, "Circular on Digital payments and PSP Regulation," Dhaka, 2021. 10.29338/psp
8. S. Karim, "Cyber Law and Financial Regulation in Bangladesh," Bangladesh Law Review , vol. 14, no. 2, pp. 97-128, 2020. 10.46985/jms.v4i1.192
9. B. Police, "Cybercrime investigation Manual," Criminal Investigation Department, Bangladesh, 2021. 10.1093/law/9780198870968.003.0017
10. A. Rahman, "Challenges of Digital Evidence in Criminal Trials," Dhaka Law Review, vol. 6, no. 1, pp. 33-61, 2019. 10.1163/15718123-bja10110
11. S. C. o. Bangladesh, Selected Judgements on Digital Evidence, Dhaka: Dhaka Law Review , 2019. 10.59619/ej.5.2.6
12. UNDP, "Justice Sector Capacity and Digital Crime," United Nations Development Progamme, Bangladesh, 2021. 10.18356/15649563-19
13. T. Islam, "Institutional Coordination in Cybercrime Enforcement," South Asian Journal of Governance , vol. 9, no. 2, p. 120, 2022. 10.2307/j.ctv3029sfz.8
14. TIB, "Annual Report," Transparency International Bangladesh , 2020-2021. 10.5337/2021.210
15. OECD, "Policy Framework on Digital Security," OECD, Paris, 2022. 10.1787/a69df866-en
16. W. Bank, "Building Trust in Digital Finance Services," World Bank, Washington DC, 2022. 10.23846/dpw1ie112
17. B. L. Comission, "Law Reforms Proposals on Cyber and Digital Crimes," Bangladesh Law Comission, Dhaka, 2020. 10.46282/blr.2017.1.1.63
18. F. S. Board, "Supervisory Technology and Risk-Based Regulation," Basel, 2020. 10.47473/2020rmm0157
19. A. D. Bank, Digital Governance and Regulatory Innovation, Manila: ADB, 2022. 10.4324/9781003347088-4