Regulating E-commerce for Consumer Protection: Lessons from Bangladesh and Global Best Practices

Professor Suborna Barua, PhD
sbarua@du.ac.bd

Tasnimussaad Abdullah

University of Dhaka
Bangladesh

ASIAN THINK TANK NETWORK FORUM 2025
Tokyo | ADB | 28-30 October

Wednesday, October 29, 2025

The Daily Star

Home | News | Opinion | Slow Reads | Sports | Business | Entertainment | Life & Living | Tech & Startup | Multi

BUSINESS

Customers still chasing refunds after e-commerce scams

Tk 58cr stuck in payment gateways as government efforts stall


Refayet Ullah Mirdha, Sukanta Halder

Thu Oct 2, 2025 12:00 AM

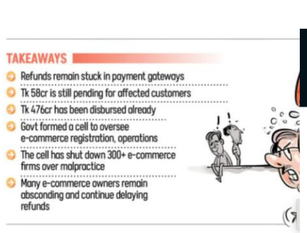
Last update on: Thu Oct 2, 2025 11:11 AM

87 Shares

Most Viewed

1 '90% of garment workers dress modestly; have we told them to wear burqas?'

2 Graffiti book, not altered map, gifted to Pakistani general: CA's office



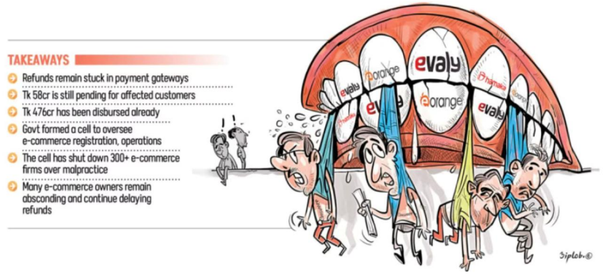
ANN ASIA NEWS NETWORK BRINGING ASIA CLOSER

HOME | AROUND ASIA | GEOPOLITICS | IN-DEPTH | BUSINESS | OPINION

Four years on, customers still chasing refunds a scams in Bangladesh

During the Covid pandemic lockdowns in 2020, online shopping gained huge popularity in eOrange, Evaly, Qcoom and Alesha Mart collecting huge sums in advance from customers prices. Instead, they reportedly siphoned off thousands of crores of takas.

Refayet Ullah Mirdha, Sukanta Halder
The Daily Star



THE BUSINESS STANDARD Wednesday October 29, 2025

Latest | Economy | Videos | World+Biz | Features | Subscribe | More | বাংলা | TBS+

AVIATION

TBS Report
16 October, 2025, 12:15 am
Last modified: 16 October, 2025, 04:15 pm

Another scam: Online travel agency Fly Far vanishes with advance payments, say customers

Customers allege the company lured them with attractive, often 'unbelievable', discounts on air tickets, hotel bookings, and international travel packages for the upcoming holiday season, thereby swindling them out of lakhs of taka.

RELATED NEWS

- 12 accused in Tk568cr market development fund embezzlement case granted bail upon surrender
- How a man named Chen Zhi carried out US and UK of large-scale scam operations
- Yet another online travel agency allegedly disappears with clients' money
- Fake ads, WhatsApp groups and bogus apps: Dismislab report sheds light on stock fraud in Bangladesh
- Excessive airport surcharge buries airlines under debt

Top Stories

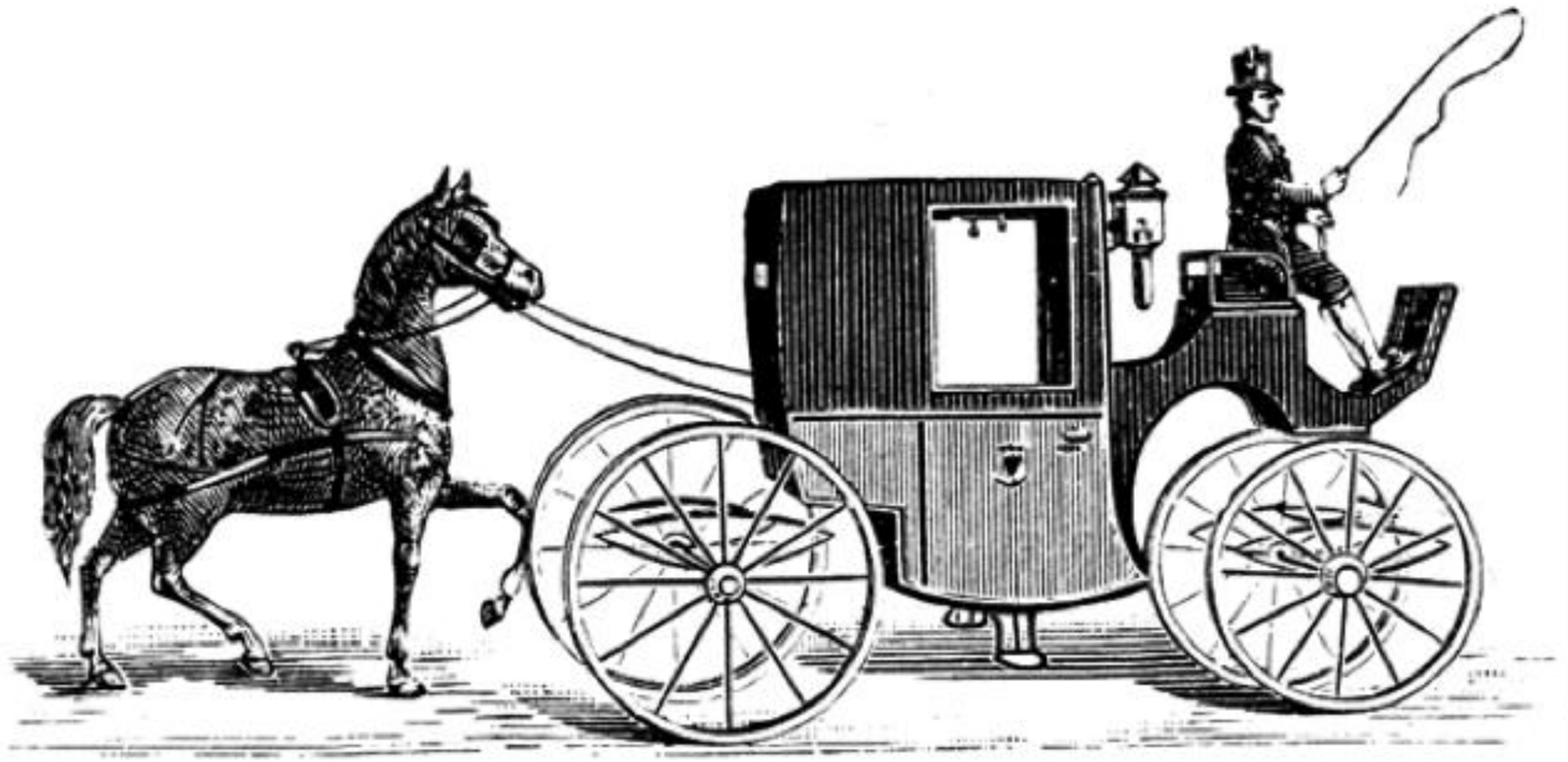
- Why proposed July charter implementation order draws concerns?
- IMF team arrives in Dhaka today to review progress on loan conditions
- Consensus Commission attempting to create 'national discord' instead of unity: Salahuddin

FLY FAR International

SPECIAL REPORTS

Double-click to read

This isn't working at all... I should warn others not to put their cart before the horse.



Overview

Introduction	1
Problem	2
Literature Review	3
Methodology	5
Overview of the Cases	6
FINRA Classification	8
Findings	9
Regulatory Gaps & Challenges	11
Global Best Practices	12
Similar Socio-Economic Structure Models	13
Lessons for Bangladesh	14

Introduction

E-commerce fraud in Bangladesh between 2015 and 2025 led to the collapse of 19 major platforms, resulting in financial losses of over BDT 5,000 crore (approximately USD 500 million) and impacting hundreds of thousands of consumers. This crisis exposed significant weaknesses in the country's regulatory framework and enforcement capacities amid rapid market growth, with Bangladesh's e-commerce sector expected to reach US$7.5 billion in 2024.

Widespread cybersecurity vulnerabilities and limited consumer protection allowed sophisticated Ponzi-style schemes to flourish, particularly through mobile financial service integrations. This study analyzes these systemic failures and major fraud cases to provide evidence-based recommendations for strengthening regulation and consumer trust in Bangladesh's digital marketplace.

Problem

The problem addressed in this paper is the widespread e-commerce fraud in Bangladesh between 2015 and 2025, which exposed critical failures in regulatory frameworks, enforcement mechanisms, and cybersecurity measures.

Despite rapid growth in the digital marketplace, systemic vulnerabilities allowed sophisticated fraudulent schemes to operate unchecked, causing significant financial losses and undermining consumer confidence. This study seeks to analyze these regulatory and security gaps to understand how they enabled large-scale fraud and to provide actionable recommendations for protecting consumers and stabilizing the e-commerce sector in developing economies.

Literature Review

Key Academic Contributions on Bangladesh E-commerce Fraud:

- Chowdhury (2025): Legal analysis of consumer protection laws; identified overlapping jurisdictions and systemic regulatory weaknesses but lacked detailed quantitative fraud data.
- Kabir (2022): Examined adequacy of business laws to combat online fraud; found no specific laws ensuring consumer rights in e-commerce.
- Rahman (2023): Highlighted absence of specific e-commerce laws, resulting in outdated legislative application.
- Sony & Al Mamun (2023): Comparative study revealing critical regulatory gaps, including no rules on predatory pricing or cross-border e-commerce.
- Tan (2024): International comparison showing the need for harmonized legal frameworks to tackle cross-border fraud, reflecting Bangladesh's challenges.
- Rofiq (2012): Behavioral framework linking cyber-fraud perception to buyer trust reduction, offering a model for fraud impact analysis.

Literature Review (Continued)

Identified Research Gaps in E-commerce Fraud Literature:

- Lack of compiled, comprehensive, quantitative documentation of all fraud cases and financial losses.
- Minimal victim demographic profiling and recovery rate analysis across cases.
- Limited application of structured fraud classification frameworks (e.g., Stanford Taxonomy of Fraud).
- Underexplored fraud mechanisms beyond legal/regulatory perspectives.
- Scarce empirical studies on cross-border enforcement and digital payment system vulnerabilities.
- Need for integrated qualitative and quantitative methodologies for systemic analysis and policy recommendations.

Methodology

This study employed a concurrent **mixed-methods, multiple-case approach**, combining qualitative and quantitative analyses to provide both contextual depth. The qualitative component mapped the chronology, fraud mechanics, and legal trajectories of each platform, while the quantitative component measured financial losses, recovery ratios, and typological frequencies.

All cases were systematically coded using the Stanford Center on Longevity/FINRA (2015) “Framework for a Taxonomy of Fraud,” allowing consistent classification and cross-case comparison. Case selection was based on strict criteria, including operation as Bangladeshi e-commerce platforms between 2015 and 2025, official investigations or court actions for fraud, and the availability of recoverable documentary evidence.

This process identified 19 major platforms with verified financial losses ranging from lakhs to over BDT 1,000 crore. Data collection drew on multiple sources such as key informant interviews with law enforcement and regulatory officials, judicial records, media archives, and academic literature.

Limitations include unreported settlements, limited regulatory transparency, currency volatility, and survivor bias.

Cases Overview

Company Name	Founding Year	Year of Arrest/Escape	Legal Action and Status	Verified Financial Loss
24tkt	2019	2021 (Arrest)	Two arrests in October 2021	BDT 50 crore
Adyan Mart	2020	2021 (Arrest)	Four officials arrested	At least BDT 18.52 lakh
Aladinerprodip	2021	-	2022 refunds issued to customers	BDT 100 crore
Alesha Mart	2020	2024 (Legal Action)	Court froze assets in 2023; founders sentenced to 6 months imprisonment in 2024	BDT 421 crore laundered
Alif World	2022	-	Refunds issued in 2022; government canceled approval for Ponzi schemes	Unclear
Anonder Bazar	2021	2021 (Escape)	Founder fled; refunds facilitated in 2022	BDT 300 crore siphoned
Bangladesh Deal	-	-	Refunds facilitated starting March 2022	BDT 55.98 lakh
Boom Boom	-	-	Bank accounts frozen in 2021	BDT 58 crore
Dalal Plus	-	2022 (Investigation)	CID filed money laundering case	BDT 41 crore
Dhamaka Shopping	2021	2021 (Arrest)	Top officials arrested; CID confiscated assets in 2025	BDT 803.5 crore collected

FINRA CLassification

Case Name	Overview (Brief)	Stanford/FINRA Code	Classification Description	Tags
Evaly	Ponzi-style e-commerce fraud with undelivered goods and refund delays.	1.2.1.2.1	Consumer Products and Services Fraud > Worthless or Non-existent Products > Paid Never Received > Online Marketplace Fraud	PZ, Ad:IE, PS:I, MT:M
E-orange	Family-led embezzlement scheme via e-commerce discounts and fake deliveries.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Qcoom	Heavy motorcycle discounts, delivery failures, escrow fund mismanagement.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Dhamaka Shopping	Operated without license, mass non-delivery, refund cheque frauds.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Aladinerprodip	Student-led Ponzi scheme, advance payments without delivery.	1.1.3	Consumer Investment Fraud > Other Investment Opportunities Fraud	PZ, Ad:IE, PS:I, MT:M
Sirajganj Shop	Fraud via mobile financial service platform (MFS), mass refunds exploited.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Alesha Mart	Unsustainable discounts, refund cheque bounce, over 100 cases.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Dalal Plus	Shell company use to embezzle large sums from customers via failed deliveries.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
24tkt	Sold fake air tickets by exploiting travel agent trust network.	1.2.2.15	Consumer Products and Services Fraud > Worthless or Non-existent Services > Travel Booking Scam	Ad:IE, PS:I, MT:M

Cases Overview (Continued)

Case Name	Overview (Brief)	Stanford/FINRA Code	Classification Description	Tags
Boom Boom	Small-scale platform, gateway fraud, part of larger laundering cases.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Anonder Bazar	Used hundi for laundering; near-total loss of deposits.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Tholay.com / WeCoom.com	Twin platforms embezzling via fake delivery promises.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Alif World	MLM-based fraud with e-commerce front; some partial refunds.	1.3.1.1	Employment Fraud > Business Opportunities Fraud > Multi-level Marketing Scheme	PS, Ad:IE, PS:I, MT:M
Bangladesh Deal	Smaller-scale fraud, failed delivery after full payments.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Sophectic	Ponzi-style platform disguised as e-commerce investment.	1.1.3	Consumer Investment Fraud > Other Investment Opportunities Fraud	Ad:IE, PS:I, MT:M
RingID	MLM-styled digital Ponzi scheme under “advertisement income” promise.	1.1.1.1.3	Securities Fraud > Equity Investment Fraud > High-Yield Investment Program (HYIP) Fraud	PZ, PS, Ad:IE, PS:I, MT:M
Adyan Mart	Regional fraud ring, heavy promotions, no product delivery.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
SPC World Express	MLM-to-e-commerce shift; swindled crores via investment pyramid scheme.	1.1.3	Consumer Investment Fraud > Other Investment Opportunities Fraud	PZ, PS, Ad:IE, PS:I, MT:M
Nirapadshop.com	Targeted students with fake 50% discount electronics offers.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M

Cases Overview (Continued)

Case Name	Overview (Brief)	Stanford/FINRA Code	Classification Description	Tags
Boom Boom	Small-scale platform, gateway fraud, part of larger laundering cases.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Anonder Bazar	Used hundi for laundering; near-total loss of deposits.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Tholay.com / WeCoom.com	Twin platforms embezzling via fake delivery promises.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Alif World	MLM-based fraud with e-commerce front; some partial refunds.	1.3.1.1	Employment Fraud > Business Opportunities Fraud > Multi-level Marketing Scheme	PS, Ad:IE, PS:I, MT:M
Bangladesh Deal	Smaller-scale fraud, failed delivery after full payments.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
Sophectic	Ponzi-style platform disguised as e-commerce investment.	1.1.3	Consumer Investment Fraud > Other Investment Opportunities Fraud	Ad:IE, PS:I, MT:M
RingID	MLM-styled digital Ponzi scheme under “advertisement income” promise.	1.1.1.1.3	Securities Fraud > Equity Investment Fraud > High-Yield Investment Program (HYIP) Fraud	PZ, PS, Ad:IE, PS:I, MT:M
Adyan Mart	Regional fraud ring, heavy promotions, no product delivery.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M
SPC World Express	MLM-to-e-commerce shift; swindled crores via investment pyramid scheme.	1.1.3	Consumer Investment Fraud > Other Investment Opportunities Fraud	PZ, PS, Ad:IE, PS:I, MT:M
Nirapadshop.com	Targeted students with fake 50% discount electronics offers.	1.2.1.2.1	Same as above	Ad:IE, PS:I, MT:M

Findings: Key Patterns of Fraud

- Most fraudulent platforms operated as **Ponzi-like schemes**, offering unrealistic discounts of 30% to 150% below market prices, making legitimate profits impossible. New customer funds were used to pay existing orders, as seen with Evaly and Qcoom, resulting in extended delivery delays and eventual collapse.

- Significant **regulatory arbitrage** allowed platforms to exploit legal gaps, using shell companies, unregistered operations, and manipulating payment gateways (e.g., Qcoom with Foster Payments, Sirajganj Shop with Nagad mobile financial service). Cross-border money laundering and founder escapes (e.g., RingID to Canada, Dhamaka Shopping to the USA) demonstrated enforcement challenges.

- Social engineering tactics **exploited cultural trust and networks**; platforms recruited journalists, leveraged university communities, and targeted expatriates with remittance-linked schemes. Artificial urgency and MLM-style investment promises coerced customers into advance payments.

Findings: Key Patterns of Fraud

- **Technology enabled** complex fraud through multiple banking accounts, diverse payment providers, and sophisticated customer targeting to avoid detection thresholds.

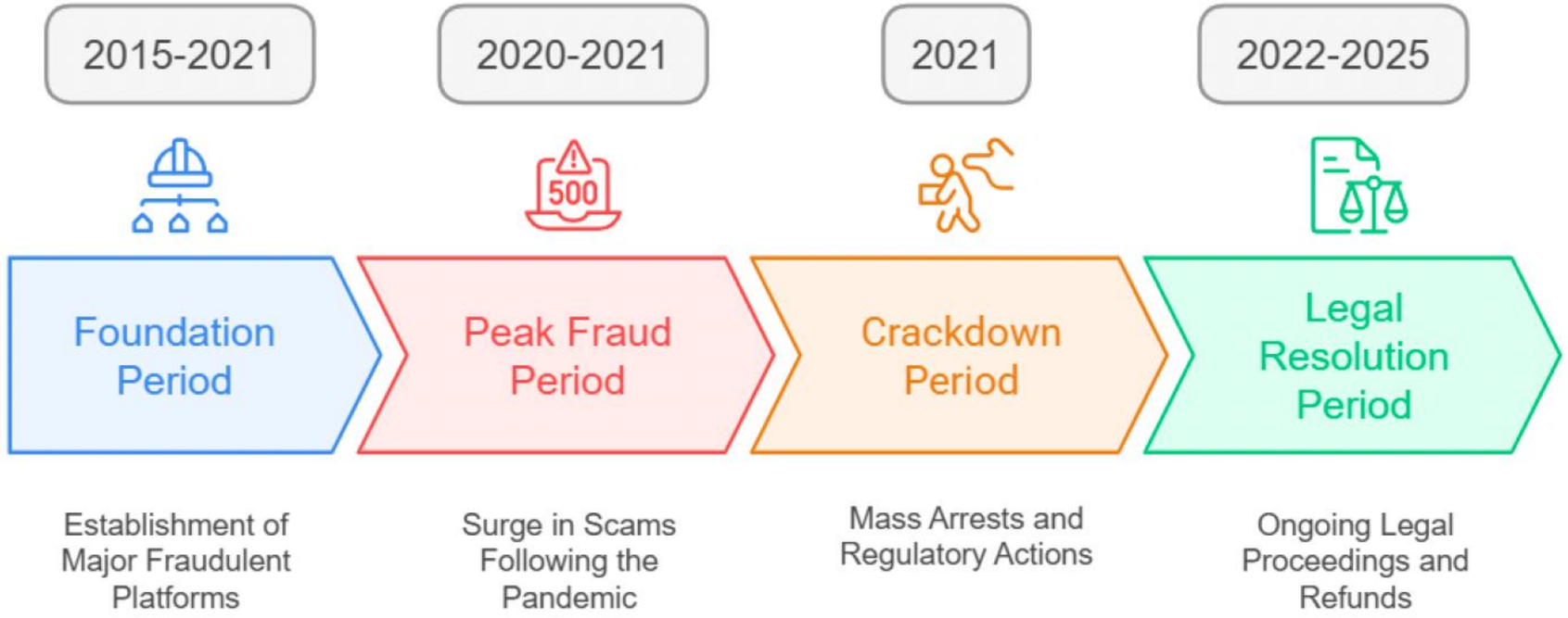
- A particularly notable pattern was the prevalence of **family-based criminal networks.** One of the platforms was controlled by a family structure, comprising the owner, her police inspector brother (provided protection), her husband (served as an advisor), and her sister-in-law (the company owner).

- **Systematic Customer Behavior Manipulation** takes advantage of consumer psychology and digital payment behavior. Fraudulent platforms offered extraordinary discounts to overcome the cash-on-delivery preference and persuaded customers to pay in advance. Platforms like RingID and SPC World Express blurred the lines between e-commerce and investment and employment schemes.

- **Regulatory Response Evolution went through Systemic Learning,** with coordinated efforts from Bangladesh Bank, CID, and the Commerce Ministry - introducing escrow services, monitoring cells, and DBID. However, **low recovery rates** and **cross-border enforcement** remain critical challenges.

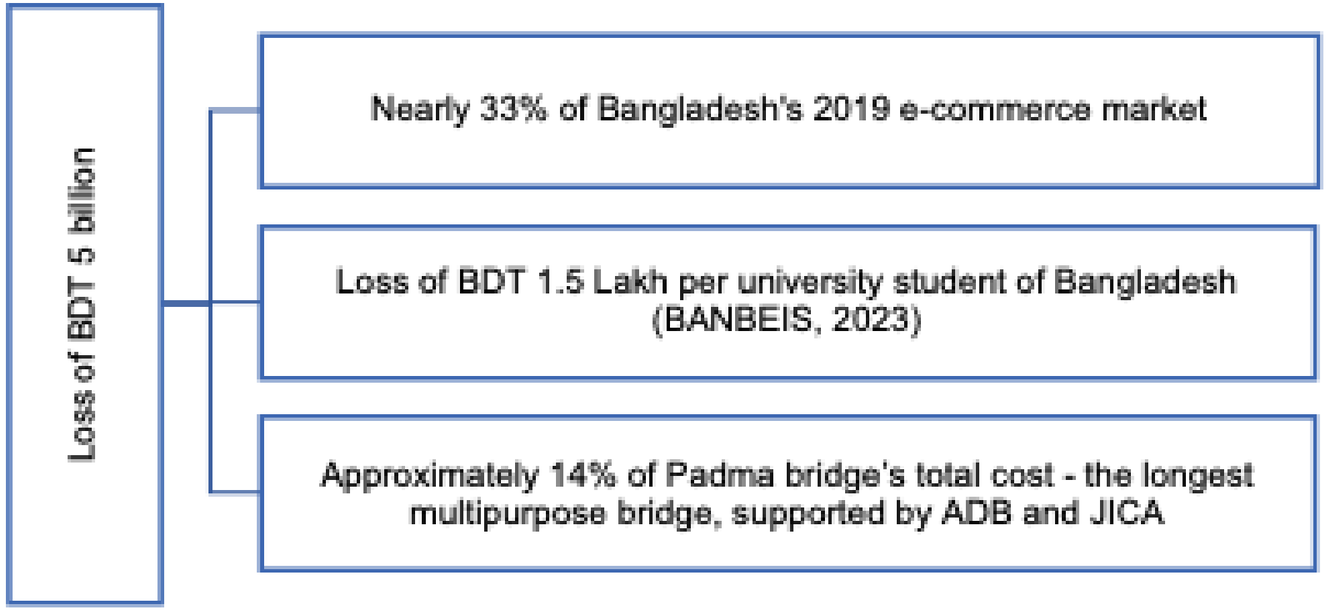
Findings: Evolution of Fraud Schemes

- **The fraud epidemic followed a timeline: foundation period (2015-2021), peak fraud period (2020-2021), crackdown (October 2021), and ongoing legal resolution (2022-2025).**



Findings: Economic Value of Frauds

- **Conservative estimates suggest cumulative losses of around BDT 5,000 crore (~33% of the 2019 market size), severely damaging consumer trust, reversing digital payment adoption, and disproportionately affecting vulnerable groups like students and expatriates.**



Regulatory Evolution

Regulatory Aspect	Pre-2021: Fragmented Framework	Post-2021: Digital Commerce Guidelines 2021
Legal Basis	Multiple outdated laws (Consumer Rights 2009, ICT Act 2006, Contract Act 1872, Sale of Goods Act 1930); no unified e-commerce law	Cyber Security Act, 2023, the Digital Commerce Operational Guidelines, 2021, National Digital Commerce Policy 2018 (amended 2020)
Business Registration	No mandatory registration or licensing; thousands of unregistered F-commerce pages	Mandatory trade license + Unique Business ID (UBID); display required on websites
Consumer Protection	Weak enforcement; limited penalties (max BDT 200,000); no grievance timeline	Complaint resolution within 72 hours; structured redress system
Delivery Standards	No delivery timelines; frequent delays	Must deliver within 5 days (city) / 10 days (inter-city)
Transparency & Product Info	Inconsistent product descriptions; misleading ads common	Mandatory clear product details, pricing, images, origin
Data Privacy & Consent	No data protection provisions	Platforms must obtain explicit user consent; disclose data usage (not yet GDPR-level)
Payment Systems	Weak oversight of digital wallets and payment gateways	All payment innovations require Bangladesh Bank approval
Social Media Commerce (F-Commerce)	Entirely unregulated (≈ 300,000 pages; > BDT 1,000 crore turnover)	Must register and comply with licensing & consumer rules
Cross-border E-Commerce	No clear framework	Foreign platforms must register locally
Regulatory Agencies	Fragmented (MoC, BB, ICT Division, DNCRP); poor coordination	MoC leads; integration with BB & other bodies under unified policy
Prohibited Activities	Not defined	Explicit bans on gambling, illegal drugs, unlicensed pharma, etc.

Regulatory Evolution

Cyber Security Act 2023

- The Cybersecurity Act 2023 replaced the Digital Security Act 2018, introducing specific provisions for digital fraud, cyberterrorism, identity theft, and unauthorized electronic transactions. The Act includes penalties of up to 14 years' imprisonment and fines of up to BDT 1 crore for serious cybercrimes (*International Center for Not-for-Profit Law,* 2024).

- *E-transaction Security Provisions:* Section 30 specifically addresses unauthorized e-transactions from financial institutions and mobile financial services, with fines up to BDT 25 lakh. However, enforcement remains challenging due to technical complexities and jurisdictional issues (*International Center for Not-for-Profit Law,* 2024).

Digital Commerce Policy 2021

- ensures a secure, transparent, and consumer-friendly e-commerce ecosystem by addressing fraud, data privacy, and fair competition. It mandates business registration, refund transparency, and data security while promoting SME participation, women entrepreneurship, cross-border e-commerce, and alignment with *Digital Bangladesh* for inclusive digital growth.

Personal Data Protection Ordinance (PDPO) 2025

- To regulate the collection and use of personal data by establishing principles for lawful, fair, and transparent processing. Key considerations include Individual rights, provisions for data processors and fiduciaries domiciled or operating in Bangladesh, data localization requirements, data breaches, and the establishment of a Data Protection Board to oversee compliance.

Regulatory Evolution

Draft Digital Commerce Authority Act 2023 proposes to regulate digital commerce by establishing a dedicated authority to register digital businesses, handle complaints, monitor online trade, and enforce penalties for misleading advertising, delivery failures, and unregistered operations—aiming to provide accountability and consumer protection in the e-commerce sector.

Key features included: the establishment of a Digital Commerce Authority (DCA), Mandatory registration, and Stringent consumer protection measures.

Draft Cross-Border Digital Commerce Policy (2024)
This focuses specifically on integrating Bangladesh's e-commerce ecosystem with the global digital marketplace and facilitating international trade.
Key objectives include:

- **Globally accepted payment system**: Implementing an international payment system connected to existing domestic systems.
- **Supporting small businesses**: Simplifying policies to assist cottage, micro, small, and medium enterprises (CMSMEs) with exporting smaller parcels.
- **Export incentives**: Providing financial incentives for digital commerce exports, similar to traditional export subsidies.
- **Prohibited goods**: Banning the cross-border trade of counterfeit products, gambling tokens, and other restricted items.

Key Regulatory Gaps Identified

Jurisdictional Overlaps & Coordination Failures

- Multiple regulators (DNCRP, BTRC, Bangladesh Bank, MoC) operate with **overlapping or unclear mandates**.
- **DNCRP** under-resourced → 12,000 complaints (2023) but few resolved; lacks digital-fraud analysts.
- **BTRC** regulates telecom infra but not F-commerce (> 500k SME pages on social media).
- **Bangladesh Bank** manages payment systems but has no standard refund rules for e-commerce.

Mobile Financial Services (MFS) Vulnerabilities

- *Fraud rates: 6.3% (users), 17% (agents), 1.6% (merchants).
- *Losses BDT 53 – 376,000 per case; ~USD 7.8 bn laundered (2022).
- *Crimes: extortion (52.6%), phone/SMS scams (42.1%), hacking (12.3%).
- **Bangladesh Bank oversight is weak**, with poor fraud detection & prevention.

Weak Legal Enforcement

- **Penalties too small** vs. large-scale fraud losses (billions BDT).
- **Cross-border fraud** and fund-recovery mechanisms are absent.
- **F-commerce** transactions (~BDT 1,000 crore/yr) remain outside formal oversight.

Social Media Commerce (F-commerce) Regulatory Void

- ~300k Facebook pages, > BDT 1,000 crore transactions per year.
- **No registration, tax compliance, or consumer protection**.
- Issues: fraud, harassment, poor quality, price manipulation.
- Only ~100 businesses linked to E-Commerce Association of Bangladesh.

**Transparency International Bangladesh, 2025*

Global Best Practices

United States of America: A multi-agency federal approach led by the **FTC** uses legislation such as the **Computer Fraud and Abuse Act, CAN-SPAM Act, and Restore Online Shoppers' Confidence Act (ROSCA)** to combat e-commerce fraud. Enforcement tools include a national fraud complaint database (Consumer Sentinel), timely delivery rules, and mandatory credit card security standards (PCI DSS). The recent **INFORM Consumers Act** requires disclosure of seller information to tackle counterfeit and fraud in online marketplaces.

European Union: The **Digital Services Act (DSA)** enforces platform liability by requiring Know Your Business Customer (KYB) protocols, proactive fraud monitoring, and notice-and-action systems with trusted flaggers. The **GDPR** enforces strict data privacy while enabling AI-enabled fraud detection**. The Payment Services Regulation (PSR)** mandates reimbursement for victims of impersonation fraud. Non-compliance can lead to fines up to 6% of the company's global annual gross revenues.

China: The **2019 E-commerce Law** prohibits discriminatory pricing, mandates platform liability for counterfeit goods, and requires explicit consent for data usage. The **2024 Consumer Protection Regulations** target the use of forged data and unfair sales practices. The **Cybersecurity Law** requires data localization and real-name verification, facilitating law enforcement cooperation. The **State Administration for Market Regulation** enforces penalties and facilitates cross-border collaboration, with asset-freezing powers for fraud cases.

Similar Socio-Economic Structure Models

India: The **Consumer Protection Act 2019** mandates e-commerce platforms to resolve complaints within 30 days, requires detailed seller disclosures, and holds platforms liable for third-party seller violations. The **2020 E-commerce Rules** enforce transparency in seller information, return policies, and prohibit misleading advertisements. The **Information Technology Act 2000** addresses identity theft, cheating, and cyber fraud with penalties including imprisonment. The **Digital Personal Data Protection Act 2023** enforces strict data privacy standards to prevent breaches and fraud.

Vietnam: The **Draft E-commerce Law 2025** focuses on platform accountability by requiring seller identity verification, content screening, and local representation for foreign platforms. **Consumer Protection Law** mandates safeguarding transaction data, seller contact disclosure, and clear return/refund policies. Cross-border regulations demand foreign platforms register locally and comply with Vietnamese standards. Platforms bear joint liability for legal non-compliance, causing consumer harm.

Philippines: The **Anti-Financial Account Scamming Act (AFASA) 2024** introduces mandatory fraud monitoring for financial institutions, enhances cybercrime investigation powers, and criminalizes money muling. The **Internet Transactions Act 2023** establishes an online business registry, grants consumers damage claims rights, and enforces platform liability. Fraud prevention is reinforced by **the Cybercrime Prevention Act 2012, Electronic Commerce Act 2000, and extended consumer protections under the Consumer Act**, combining comprehensive legal tools for digital fraud deterrence.

Key Lessons for Bangladesh

- **Enact a unified E-commerce Consumer Protection and Fraud Prevention Act** to consolidate regulations under a single empowered authority, eliminating legal fragmentation.
- **Implement enhanced platform accountability with tiered liability**, requiring seller verification, active transaction monitoring, and victim compensation, modeled on the EU and China.
- **Mandate AI-driven, real-time fraud detection systems** across e-commerce and Mobile Financial Services, enabling instant alerts and automatic blocking of suspicious activities.
- **Strengthen cybersecurity and digital financial safeguards**, addressing vulnerabilities in platforms and MFS to prevent hacking, credential theft, and internal embezzlement.
- **Develop cross-border enforcement frameworks requiring foreign platforms to have local presence**, comply with national laws, and engage in mutual legal assistance.
- **Regulate social media commerce (F-commerce)** with mandatory seller verification, transaction tracking, and enforceable consumer protections to mitigate unregulated risks.

Thank you

Any Questions?