The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/1368-5201.htm

Is Bangladesh's policy response to the growing e-commerce sector compatible with its commitment to fight predicate offences for money laundering?

Md. Zahurul Haq
School of Law, Universiti Utara Malaysia, Sintok, Malaysia

Abstract

Purpose – This study aims to investigate Bangladesh's e-commerce regulations in light of the growing criticism that they are insufficient to curb predicate crimes like fraud and money laundering in the online marketplace.

Design/methodology/approach – This study used the exploratory design to examine the latest ministerial directives and laws governing e-commerce in Bangladesh to determine why they cannot prevent fraudulent activities in this promising sector and identify potential solutions.

Findings – Bangladesh's regulatory responses to e-commerce fraud prevention and detection are reactive and inadequate. Regulators are unwilling and unable to enforce available legal provisions for various reasons, including a lack of knowledge and coordination among the agencies.

Research limitations/implications – This paper focuses solely on the legal and regulatory framework in place to combat e-commerce fraud. Other critical issues, such as consumer rights, privacy and data protection in e-commerce, are not addressed.

Practical implications – The findings of this study will assist policymakers in revising current regulatory approaches to e-commerce to protect this sector from criminal abuse.

Originality/value – This study looked into the possibility of using a proactive risk-based approach in the e-commerce sector, similar to what the Bangladesh Financial Intelligence Unit does in the financial sector.

Keywords E-commerce, Bangladesh, Money laundering, Fraud, E-commerce policy

Paper type Research paper

1. Introduction

Between March and June 2021, 25 e-commerce platforms in Bangladesh were inundated with orders totalling Taka 6,050 crore (approximately US$728.91m as of March 2021), thanks to Ponzi-like swindles that enticed naïve buyers with substantial discounts. The central bank detected the alleged scams during an investigation that also revealed the enormous scope of fraud within the growing e-commerce sector in the country. Typically, monthly transactions for this sector range from Taka Taka 500 to Taka 550 crore (approximately US$60.24–66.26m as of March 2021) (Uddin and Hasan, 2022).

Until March 2021, Evaly – one of the e-commerce platforms involved in the alleged scam – owed its customers and suppliers around Taka 403.8 crore (US$48.65m as of March 2021) while it held assets worth a total of over Taka 65 crore (US$7.83m as of March 2021) only. Most of its customers had been waiting months for their orders to arrive, and only a fraction of them was offered reimbursements as a credit on the platform's unlicensed digital wallet

Journal of Money Laundering Control
Vol. 27 No. 3, 2024
pp. 520-531
© Emerald Publishing Limited
1368-5201
DOI 10.1108/JMLC-01-2023-0023

(The Daily Star, 2021a, 16 August 2021). As immediate measures, the Directorate of National Consumer Rights Protection fined 17 e-commerce platforms for the non-delivery of products and for deceiving customers through false advertisements as more incidents unfolded (The Daily Star, 2021b, 18 October 2021).

The alleged scams occurred when the National Digital Commerce Policy, 2018 (after this Policy) was already in force, requiring all e-commerce platforms to comply with relevant laws on electronic transactions and consumer protection, among others. The Policy required a central body to be formed under the ministry of commerce to oversee compliance with its provisions (Ministry of Commerce, 2018, Clauses 3.1–3.3). This body would coordinate with financial institutions, clearing houses and law enforcement agencies to prevent any misuse of the electronic payment system, including fraud (Ministry of Commerce, 2018, Clause 3.7.3). For example, the Policy proposed that all financial transactions be carried out indirectly via an escrow account under the central bank's supervision to reduce the potential risk of transaction fraud (Ministry of Commerce, 2018, Clause 3.3.7).

However, some e-commerce platforms that mushroomed over the last few years remained obstinate in their attitude towards even the most basic regulatory provisions. This was possible mainly because the authorities did not activate the central body or introduce escrow services until July 2021 (Liaquat, 2021), providing enormous opportunities for fraudsters. Subsequently, in the wake of intense criticism from the public, the Government formed three committees to review the existing e-commerce policies and practices. Its immediate outcome was releasing the Digital Commerce Operating Guideline (2021) (after this 2021 Guideline) by the ministry of commerce to reinforce existing rules on e-commerce (The Daily Star, 2021b, 18 October 2021).

It was a positive move, but the 2021 Guideline, like the Policy, offered no promising solution to the ongoing problem. It did not identify any specific anti-fraud provisions in the relevant laws that might apply in the electronic environment. What it means, among other things, is that an ideal environment exists to facilitate transaction laundering, where unknown illicit businesses can easily process payments through known merchants. Therefore, the e-commerce sector in Bangladesh remains unprotected against financial crimes, saddled with inadequate regulatory provisions and low consumer rights protection. If the authorities do not provide adequate regulatory oversight, this promising sector may soon become a conduit for financial crime.

Provisions of the Policy, the 2021 Guideline and all Acts except the Penal Code and the Sale of Goods Act used in this article are translated from the source language Bangla.

1.1 Growth of the e-commerce sector in Bangladesh

The internet first appeared in Bangladesh in the 1990s. As of August 2022, there are 127.26 million subscribers (BTRC, 2022), which is about 75.65% of the country's nearly 168.22 million people (BBS, 2022, p. XXII). This indicates that e-commerce has enormous potential in this country. Since its inception in 2015, the e-Commerce Association of Bangladesh has registered over 1,800 e-commerce businesses as members. At this stage, it was essential to bring this promising sector under regulation. Inspired by the eTrade for all initiative, launched at the fourteenth Ministerial Conference of the United Nations Conference on Trade and Development in July 2016, the Ministry of Commerce's World Trade Organization cell developed the National Digital Commerce Policy in 2018. The Policy's primary goal was to promote an environment conducive to e-commerce in Bangladesh by supporting its sustainable development and implementing control and oversight mechanisms (Ministry of Commerce, 2018, pp. 854–855).

2. An overview of the Policy

The Policy has three chapters covering its scope and definitions (Chapter I), objectives (Chapter II) and operation and management of digital commerce (Chapter III). Three essential characteristics of this executive instrument are that it is inexcusably brief, deliberately vague and nonbinding. For example, it introduces the concept of a central policy implementation body (central body) in two lines without defining its formation, the scope of work and power, among others (Ministry of Commerce, 2018, Clause 3.1.1). Similarly, "businesses organisations shall comply with all relevant rules and regulations of the country in e-commerce business operation" (Ministry of Commerce, 2018, Clause 3.1.2), or "e-commerce entities shall ensure that customers" personal data is protected' (Ministry of Commerce, 2018, Clause 3.6.9) are highly ambiguous. There is no privacy and data protection law in the country to comply with the constitutional guarantee of privacy (Constitution of the People's Republic of Bangladesh, 1972, Article 43). Besides, the Policy does not come with the binding force of the law. It is an executive instrument. Its language is more like advice or suggestion as it is not addressed to any specific person or body and does not attach adverse legal or procedural consequences to a party's noncompliance.

The Policy contains several provisions to protect the buyers by prohibiting fraud and indirectly establishing punishment for those who defraud others. These provisions are not mentioned as such, but if someone violates relevant laws of the country, law enforcement agencies can bring appropriate enforcement actions. But it is unclear if the central body under the ministry of commerce or individual victims may sue those who have defrauded them. Chapter III of the Policy contains several anti-fraud clauses. The researcher classified them into three broad categories – definition of fraud, prohibition on anonymity and protection of electronic transactions – based on their intended role in preventing fraudulent activities on the e-commerce platforms.

2.1 Definition of fraud

Clause 3.7.3 contains the Policy's most explicit anti-fraud provision. It states that:

> [. . .] financial institutions, clearing houses, and law enforcement agencies must take the necessary measures in coordination with the central digital commerce cell (central body) to detect fraud and abuse of electronic transaction systems (Ministry of Commerce, 2018).

To explain "fraud" in the electronic environment, the Policy refers to "laws related to digital security" (3.6.1), which is the interpretative note to section 23 of the Digital Security Act (2018). As stated in this note:

> Digital or electronic fraud means intentionally or knowingly or without permission altering, deleting, reducing the value or utility of information through the addition or distortion of data in a computer programme, computer system, computer network, digital device, digital system, digital network, or any social media platform by a person, an attempt to gain an advantage for himself or another person, cause harm, or resort to deception.

However, it is unclear how "[. . .] intentionally or knowingly or without permission altering, deleting, reducing the value or utility of information [. . .] by a person" could be interpreted for identifying essential elements of common law fraud. Through an "intentional" act (or omission), a wrongdoer may create a representation of fact (St. Louis S. F. R. Co. v. Reed, 37 Okla. 350, 132 P. 355, Okla 1913), but if such an act or omission does not demonstrate the falsity of the representation (BLAU v. America's servicing company, 2009), or operates as an inducement to the plaintiff to enter into a contract (Prudential Ins. Co. of America v. Anaya, 1967), then two of the primary elements of common law fraud are not established. Similarly,

"[t]he fundamental character of fraud is the communication of a misimpression to induce another to rely on it" (Estate of Schwarz v. Philip Morris, Inc., 2006). Suppose the representer's intention to induce the plaintiff to act on the said representation is not established, and the plaintiff did not actually rely on the truth of the representation (Spinks v. Clark, 147Cal. 439, 82P. 45, Cal. 1905), and suffered consequences (Stokes v. Victory Land Co., 1930). In that case, no fraud is established (Mitchell, 2022). Therefore, "an attempt to gain an advantage for himself or another person, cause harm" fall far short of the minimum requirement for an action to amount to fraud, especially when the last two phrases are independent of the rest of the clause.

Furthermore, this interpretative note on fraud diverges too far from the most relevant penal provision of the country. Section 415 of the Penal Code, 1860, defines cheating as:

> Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

In a common law fraud claim, a plaintiff must plead with specificity and particularity that the defendant purposefully or recklessly represented material and false fact with the intent to cause the plaintiff to act following the representation and that the plaintiff relied upon the said representation to his injury (Horvath *et al.*, 2009, pp. 541–542, Mitchell, 2022). Thus, except for "resort to deception" and, in some instances, "an attempt to gain an advantage for himself or another person, cause harm," both being independent parts of the interpretative note, no other parts even remotely refer to fraud. The problem remained unchanged under the 2021 Guidelines.

Despite this shortcoming, the prosecutors may trace at least three common patterns and practices of internet fraud (Montague, 2011, p. 57) in the Digital Security Act (DSA), such as identity theft (section 24 (1) a-b), social engineering (section 22) and internal fraud (section 23). Then again, DSA does not directly mention social engineering (attempting to collect information through social interactions) or internal fraud (organised fraudulent activity). Only a court's liberal interpretation of electronic forgery under section 22 (illegally changing shipping information or billing data) and an action under section 415, read with section 34 (common intention), of the Penal Code may hold an individual or group criminally liable for any of these fraudulent activities.

2.2 Prohibition of anonymity

In general, the virtual world is an appealing sector for criminals because it allows for numerous high-volume transactions in a short period of time, from any location, by anyone disguised under a borrowed name. From this vantage point, an e-commerce marketplace may be especially alluring for perpetrators of financial crimes because it may allow the sale of fake or contraband goods as well as over-inflated transactions. As a result, licencing and registration for operators are essential prerequisites of public regulation and supervision, just as they are for any other business. This is also a way regulators can prevent money launderers from using front companies to conceal their illegal activities.

Nevertheless, the Policy's reaction to this potential vulnerability is limited. While it advises the e-commerce operators to display their registration numbers on their respective websites, it does not provide additional information on obtaining such numbers (clause 3.1.4). Does this imply that a company could use its current registration information to participate in the e-marketplace? If so, does this also mean that registered pharmacy

owners can sell controlled drugs over the internet without special risk assessment and identity verification? The 2021 Guideline addressed some of these issues.

Under the 2021 Guideline, an individual or entity must register their e-commerce site either with a trade licence, a Value Added Tax registration certificate, a Unique Business Identification Number or a Personal Retail Number to demonstrate their identity (clause 3.1.12). Because the Bangladesh Financial Intelligence Unit (BFIU) discovered evidence of money laundering by e-commerce platforms (Sarkar, 2022a), one of the primary goals of this requirement was to identify online business owners and subject them to specific financial regulations to prevent money laundering. However, the policymakers wilfully disregarded the social reality that anyone may collect any of these documents with the help of a forged National Identity Document (NID). Because the NID database is inaccessible for online verification, even for many public authorities, the use of forged NID is widespread in Bangladesh (The Daily Star, 2022, 23 March 2022; The New Age, 2020; Dey and Suman, 2019).

Instead, policymakers could mandate using "reliable, independent digital ID systems with appropriate risk mitigation measures in place" (FATF, 2012, Recommendation 10 (a), FATF, 2020, p. 5), like electronic signatures. A valid electronic signature provides a high level of assurance to the consumer that the content was created by a legitimate entity and was not altered illegally. This is a widely accepted method of confirming the authenticity of digital documents. In Bangladesh, electronic records and signatures are governed by the Information and Communication Technology Act (ICT Act) (2006) (sections 5–7). Since its inception in 2010, the Controller of Certifying Authorities [Information and Communication (Certifying Authority) Rules, 2010] has issued licenses to seven Certifying Authorities (Office of the Controller of Certifying Authorities, 2022). Therefore, neither the service's legality nor availability may be used to explain its non-use.

2.3 Protection of electronic transactions

Aside from calling for action against fraudulent activity and anonymity, the Policy proposes safeguards for online transactions in e-commerce platforms. It advises complying with *relevant laws* (emphasis added) in force (clauses 3.3.1–3.3.2) to make online transactions safer. Besides, the Policy proposes introducing escrow services (clauses 3.3.7) for secure online payment processing. But the question remains to what extent are these legislative and regulatory provisions meant to guarantee the safety of electronic transactions in the e-commerce marketplace? They hardly appear innovative or futuristic, contributing to this doubt.

To begin with, the proposal for complying with *relevant laws* (emphasis added) in force is ambiguous. The primary legislation governing information technology, including computing and the internet, is the ICT Act (2006). ICT Act legalises electronic records (section 6), the use of electronic signatures (section 5) and electronic contracts (sections 13–15). Therefore, no one may deny the legal effect, validity or enforceability of any electronic signature, contract or record only because it is in electronic form. From this perspective, *all* (emphasis added) electronic transactions should enjoy the same legal protection as regular paper-based financial transactions.

However, the Act does not define "transaction" or "electronic transaction" but mentions "financial transactions" a few times (sections 8, 11–12) without further elaboration. Some partial clarity comes from the Policy, as it defines "digital payment" as "any payment made in the digital form in digital commerce" [clause 1.2 (12)]. Still, no specific e-transaction security issues, their elements and relations are mentioned anywhere in the Policy or 2021 Guideline. Thus, identifying a set of *relevant* (emphasis added) anti-threat legal provisions to which the Policy refers will be hypothetical in the absence of precedent. Suppose "errors" in

the electronic fund transfer process is a security issue. The relevant regulatory framework might be the Bangladesh Electronic Funds Transfer Network (BEFTN) Operating Rules (2010), promulgated by the central bank.

BEFTN facilitates businesses and consumers engaged in e-commerce (BEFTN, 2010, p. 5) and prescribes the procedure to follow if an error occurs (BEFTN, 2010, p. 37) in electronic fund transfer attempts. But the Rules were created for Banking institutions long before any regulatory framework existed for e-commerce in Bangladesh. Therefore, there is ample doubt if the said procedure will lead to the expected outcome when applied to a business-to-consumer scenario involving natural persons. There are at least two reasons behind this uncertainty. Firstly, neither the Policy nor the 2021 Guideline requires the e-commerce platforms to provide the appropriate means to enable the buyer to rectify transaction errors before the buyer confirms the order made. If an error occurs during a transaction, consumers will be bound by the terms and conditions of the seller.

Second, there are no provisions for who may assume the risk of any defects, delays or loss of money in the transmission if a mistake occurs due to the malfunction of an electronic agent installed by the e-commerce platform concerned. Some specific legal or regulatory provisions covering automated transactions using an electronic agent (without immediate human intervention) could provide stronger consumer protection in the electronic environment. For instance, under the Uniform Electronic Transactions Act (UETA) (1999) of the USA, if a change or error occurs in an electronic record between parties to a transaction, the following rules apply [Errors and Changes (Section 10)]:

- A person may avoid a transaction caused by an inadvertent error if, upon learning that another party believes a transaction occurred, he gives prompt notice of the error, does not use or receive a benefit from the transaction and complies with any instructions for returning or destroying any received consideration.
- If the parties agreed to use a security procedure to detect changes or errors and only one party conforms, the conforming party may avoid the effect of any error or change if the nonconforming party would have detected it if he had conformed.
- In all other instances, the change or error has the effect provided by law, including the law of mistake and the parties' contract.

The other part of the ambiguity regarding the *relevant laws'* (emphasis added) efficacy concerns the Government's legislative intent relating to the application of digital signatures. The e-contract securing system using digital signature and digital certificate is a well-established approach in traditional business relations (El-Bendary, 2011, p. 184). The certificate binds a digital signature to a specific person or entity. In contrast, the signature authenticates the message's source and assures it has not been altered in transit. A certificate provides a unique identifier for each user, which can be used to match behavioural patterns with a user's profile, control a user's access to specific services and encrypt electronic communications. Combined, they eliminate the inherent security flaws of paper-based identification documents and password implementation (Vagadia, 2020, p. 128).

Today, digital signatures use a standard format known as public key infrastructure, which has universal acceptance and provides the highest protection against online fraud (D'Angio *et al.*, 2010, p. 111). However, the Government has consistently rejected the use of digital signatures in business. Despite its legal recognition in 2006, they did not issue the Information Technology (Certifying Authority) Rules until 2010, Certifying Authority licences until 2011 and the Certificate Policy until 2012. And even after the series of recent fraudulent activities on the e-commerce platforms and the continuing failure to trace

laundered funds, the Policy remained unchanged. Identity verification is still largely paper-based because digital technology usage is optional. This prolonged process of implementation has given rise to doubt about the Government's intention to promote the common good through the enactment of the ICT Act or, in their language, "ICT-based innovative business" in "Digital Bangladesh" (Mahmood, 2022, p. 188).

A counterargument can be seen in Srivastava (2011), "Resistance to change: six reasons why businesses don't use e-signatures," which suggests a range of social, legal and technical concerns might contribute to the abandonment of electronic signatures in the e-commerce business. However, Srivastava's investigation differs in issue, objective and methods from this study. Srivastava investigated the factors that contributed to the low acceptance of electronic signatures in 27 publicly listed companies in Australia. This was a study to understand the resistance among top-listed companies to technological change (2011, pp. 357–361) who were not necessarily under scrutiny for illegal activities. Instead, it relates to the rejection of perceived conveniences of technology. Conversely, this ongoing study examines how the Government's indifference to mandating digital signatures as security measures may affect fraudulent activities in an e-commerce sector highly vulnerable to fraud (TIB, 2020; Jamil *et al.*, 2016, p. 103).

The other proposal of the Policy is to introduce escrow services to prevent fraud (clauses 3.3.7). Internet escrow protects both the buyer and seller in a trade by placing money in the hands of a licensed third party. The funds are released once both parties confirm they completed the deal as agreed. Therefore, this service could help prevent non-delivery fraud by acting as an independent third party between buyers and sellers. However, the proposed service remained unavailable until July 2021 (Liaquat, 2021), when widespread online shopping scams began to unravel (Hossain, 2021). The situation has mostly stayed the same under the 2021 Guideline since the adoption of this service is still voluntary (clause 3.5.3).

3. How does it affect the money laundering risk

Until the third round of the Asia Pacific Group (APG) on money laundering mutual evaluation, Bangladesh conducted two National Risk Assessments (NRA) and several sectoral risk assessments for money laundering and countering the financing of terrorism. The latest NRA (2015) identified five high-risk threat areas: corruption, fraud, forgery, human trafficking and smuggling, as well as the four highest-risk sectors: banking, nonbanking financial institutions, real estate and jewellery (APG, 2016, p. 19). These documents make no mention of the vulnerable e-commerce sector. One possible explanation for this omission could be that the 2016 mutual evaluation and the 2015 NRA were based on data collected before 2016 when suspected e-commerce fraud cases had not become an issue yet.

However, the claim does not justify its continuing omission in the subsequent discourses, including the 4th Follow-Up Report on the Mutual Evaluation of Bangladesh, published by the Financial Action Task Force in 2020 (FATF, 2020) and the official circulars of BFIU in 2022. This is because, following the unfolding of recent e-commerce scams, the High Court of Bangladesh ordered that the individuals and institutions responsible for scams and money laundering through e-commerce platforms be identified. The Court asked the Government and the Anti-Corruption Commission to submit separate compliance reports after determining the amount of misappropriated money. The High Court issued this order after the Court reviewed a compliance report from BFIU, which discovered evidence of fraud, suspicious financial transactions and money laundering by eight e-commerce platforms (Sarkar, 2022b).

The omission demonstrates policymakers' steadfast refusal to acknowledge the potential abuse of e-commerce as a conduit for financial crime. One of the apparent consequences of this approach was that the Government resorted to the less contentious reactive mechanism, which aimed at treating the e-commerce sector as traditional commerce. This offered some instant benefits. It helped the Government avoid implementing a costly, new and challenging regulatory regime of which they had limited knowledge. But this pseudo-benefit did not come without a cost. The Policy and the 2021 Guideline permitted a very questionable cash-on-delivery (COD) payment mechanism. It allows the buyers to receive all COD refunds directly to their nominated bank account. Although a single cash transaction may not exceed Taka 65,000.00 (US$638, as of November 2022), there is no daily or monthly transaction limit (Daraz, 2022). Therefore, the arrangement may serve as a highly convenient mechanism to provide placement services to the launderers within an approved business model. It sounds more like a textbook example of a pro-money laundering e-commerce policy.

4. The way forward

As described in the preceding sections, two significant characteristics of the anti-fraud provisions are that they are primarily reactive and ultimately self-contradictory. These are substantial weaknesses as well. Therefore, if these two weaknesses remain unaddressed, no meaningful solution to the current problem concerning fraudulent activities is likely to come.

As a member of the APG, Bangladesh is under an international obligation to comply with the FATF recommendations and to meet the shared objectives to fight money laundering. In particular, they should identify, assess and comprehend their money laundering risks and adopt a risk-based approach to ensure that measures to prevent money laundering are proportionate to the risks identified (FATF, 2012, Recommendation 1). The latest APG mutual evaluation indicates that Bangladesh has made significant progress, demonstrating its political commitment and leadership in anti-money laundering initiatives (APG, 2016, p. 3). The commendation includes a "largely compliant" rating for technical compliance with customer due diligence (CDD) and record-keeping requirements (APG, 2016, p. 176). And this means, among other things, that the BFIU has succeeded in implementing CDD measures among the reporting entities for customer identification and verification using reliable, independent source documents and identification of the beneficial owner and the businesses (FATF, 2012, Recommendation 10). While a decent achievement, there are still significant gaps in identifying and analysing money laundering threats, such as the actors, crime types, source and destination of criminal proceeds (APG, 2016, p. 175).

Yet, the experience of the successful implementation of CDD in the financial sector could help succeed the Policy against anonymity and threats to electronic transactions. The initiative may further benefit from the digital certificate and signature services if the Government makes it obligatory for businesses. Here, the proposal is not to bring the e-commerce entities under the anti-money laundering system but to use a proactive risk-based approach (FATF, 2012, Recommendation 1) alongside the present reactive measures. And, given the circumstances, the proposal to introduce a more robust identification mechanism for e-commerce actors seems more rational because Bangladesh already has reasonably solid experience in successful CDD.

Next, the Policy and the 2021 Guideline have proposed several self-contradictory stipulations. On the one hand, both instruments frequently refer to unspecified *relevant laws* (emphasis added) currently in force; on the other hand, occasionally, they refer to specific rules or offer an interpretation of legal provisions, which is confusing. For instance, the 2021 Guideline requires a seller to deliver an item to the buyers within five to 10 days, depending on the distance, following full payment (clause 3.3.2). This is an interpretation of the term

"reasonable time" as stipulated under section 36 (2) of the Sale of Goods Act, 1930 on "rule as to delivery." However, the Act mentions that the question of what a reasonable time is a "question of fact" (section 63) and needs to be determined by the judge or jury (Markman v. Westview Instruments, Inc., 1996), not by the executive power of the Government. Similar criticism also applies to the Policy's unsuccessful attempt (clause 3.6.1) to link the interpretative note to section 23 of the DSA to common law fraud defined in the Penal Code (section 2.1.1 above). In sum, while complete silence on laws – which might misinform further – would not be the ideal approach to regulating fraudulent behaviour in the e-commerce marketplace, policymakers should avoid misleading interpretations and references.

5. Conclusion

The ongoing scam involving e-commerce platforms in Bangladesh has revealed regulators' reluctance to acknowledge the problem of e-commerce fraud and called into question their ability to take action against entities involved in alleged scams, creating enormous opportunities for fraud. At the outset, the researcher argued that the current c-commerce policy's weakness lies in its inability to identify potential scopes of fraud and available legislative and regulatory responses to such offences. Understanding this fragility is essential because the continuing scam and the authorities' inability to trace the laundered funds have direct implications for consumer rights, financial crime prevention and the overall growth of this promising sector.

To date, the ongoing discourses have mainly highlighted how the fraudsters exploited the ignorance of online shoppers to perpetrate fraud; however, this study explains the loopholes in the anti-fraud legal and regulatory provisions which actually facilitated the commission of such offences. While this study does not offer an exhaustive list of all possible legal and regulatory issues relating to ongoing fraudulent activities, it identifies the core policy issues arising under the current e-commerce regulatory framework that would require the attention of the Government.

The research raises important questions about the regulator's over-emphasis on a reactive mechanism against fraud and the effect of the Government's technophobic attitude on the overall management of the e-commerce sector because paper-based transaction and identification system is less secure. Finally, the researcher proposes strengthening the current reactive approach to fraudulent activities with a proactive risk-based approach used in Bangladesh's anti-money laundering regulatory system. It would be interesting to pursue further research about the impact of the existing legislative and regulatory dilemma, as described in this study, on the outcome of the pending cases against the alleged fraudsters.

References

APG (2016), "Anti-money laundering and counter-terrorist financing measures Bangladesh mutual evaluation report", available at: www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/APG-MER-Bangladesh-2016.pdf (accessed 10 March 2021).

BBS (2022), "Statistical yearbook Bangladesh 2921", available at: http://bbs.portal.gov.bd/sites/default/files/files/bbs.portal.gov.bd/page/b2db8758_8497_412c_a9ec_6bb299f8b3ab/2022-06-15-10-49-3cf641425dd693f9e954de5ae9470775.pdf (accessed 10 October 2022).

BTRC (2022), "Internet subscriber", available at: www.btrc.gov.bd/site/page/347df7fe-409f-451e-a415-65b109a207f5/%E0%A6%87%E0%A6%A8%E0%A7%8D%E0%A6%9F%E0%A6%BE%E0%A6%B0%E0%A6%A8%E0%A7%87%E0%A6%9F-%E0%A6%97%E0%A7%8D%E0%A6%B0%E0%A6%BE%E0%A6%B9%E0%A6%95 (accessed, 10 October 2022).

Constitution of the People's Republic of Bangladesh (1972), available at: http://bdlaws.minlaw.gov.bd/act-367.html (accessed 27 September 2022).

D'Angio, P., Vassilliandas, P. and Kaklamanis, P. (2010), "'PKI – Crawling out of the grave and into the arms of government", in Pohlmann, N., Reimer, H. and Schneider, W. (Eds), *ISSE 2009 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2009 Conference*, Vieweg + Teubner, Wiesbaden, pp. 108-116.

Daraz (2022), "Return and refund", available at: https://pages.daraz.com.bd/wow/i/bd/help-pages/returns-refunds-faq?spm=a2a0e.11886594.9877735410.15.7c9e259937lknE&hybrid=1 (accessed 24 November 2022).

Dey, A.B. and Suman, M. (2019), "National identity cards: at least 73 dubious applications in EC database", *The Daily Star*, 4 September, available at: www.thedailystar.net/frontpage/73-fake-nid-card-applications-found-in-ec-database-1795075 (accessed 18 October 2022).

Digital Commerce Operating Guideline (2021), available at: https://mincom.gov.bd/site/page/c0b4167c-c61b-4092-bd59-510e53833483/%E0%A6%A1%E0%A6%BF%E0%A6%9C%E0%A6%BF%E0%A6%9F%E0%A6%BE%E0%A6%B2-%E0%A6%95%E0%A6%AE%E0%A6%BE%E0%A6%B0%E0%A7%8D%E0%A6%B8-%E0%A6%AA%E0%A6%B0%E0%A6%BF%E0%A6%9A%E0%A6%BE%E0%A6%B2%E0%A6%A8%E0%A6%BE-%E0%A6%A8%E0%A6%BF%E0%A6%B0%E0%A7%8D%E0%A6%A6%E0%A7%87%E0%A6%B6%E0%A6%BF%E0%A6%95%E0%A6%BE–%E0%A7%A8%E0%A7%A6%E0%A7%A8%E0%A7%A7 (accessed 30 November 2022).

El-Bendary, N., Snasel, V., Adam, G., Mansour, F., Ghali, N.I., Soliman, O.S. and Hassanien, A.E. (2011), "E-Contract securing system using digital signature approach", in Kim, Th., Adeli, H., Robles, R. J., Balitanas, M. (Eds), *Advanced Communication and Networking. ACN 2011, Communications in Computer and Information Science*, Springer, Berlin, Heidelberg, p. 184.

FATF (2012), "The FATF recommendations", available at: www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (accessed 25 September 2022).

FATF (2020), "4th Follow-Up report, mutual evaluation of Bangladesh", available at: www.fatf-gafi.org/media/fatf/documents/reports/fur/APG-Follow-Up-Report-Bangladesh-2020.pdf (accessed 24 November 2022).

FATF (2020), "Guidance on digital identity", available at: www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf (accessed 11 November 2022).

Horvath, A., Villafranco, J. and Calkins, S. (2009), *Consumer Protection Law Developments*, American Bar Association, Chicago.

Hossain, S. (2021), "11.48% Customers victim of online shopping scams in 2020", *The Dhaka Tribune*, 19 June, available at: https://archive.dhakatribune.com/business/commerce/2021/06/20/11-48-customers-victim-of-online-shopping-scams-in-2020 (accessed 4 November 2022).

Information and Communication Technology Act (ICT Act) (2006).

Information and Communication (Certifying Authority) Rules (2010), available at: https://ictd.gov.bd/sites/default/files/files/ictd.portal.gov.bd/law/13c94d86_d49c_4037_8f9d_0fcc77227685/CCA%20Bidhimala.pdf (accessed 18 October 2022).

Jamil, I., Askvik, S. and Hossain, F. (2016), *Administrative Culture in Developing and Transitional Countries*, Routledge, Oxon.

Liaquat, Z.B. (2021), "BB instructs payment gateways to start paying back e-commerce consumers", *The Dhaka Tribune*, 19 December, available at: www.dhakatribune.com/business/2021/12/19/bb-instructs-payment-gateways-to-start-paying-back-e-commerce-consumers (accessed 7 October 2022).

Mahmood, S.A. (2022), "Government-Business relationship in Bangladesh", in Khondker, H., Muurlink, O. and Ali, A.B. (Eds), *The Emergence of Bangladesh: Interdisciplinary Perspectives*, Palgrav, Singapore, p. 188.

Ministry of Commerce (2018), "National digital commerce policy 2018", available at: www.mincom.gov.bd/site/page/1585c28a-feb9-45e6-b82e-ea56cae59c84/%E0%A6%A1%E0%A6%BF%E0%A6%9C%E0%A6%BF%E0%A6%9F%E0%A6%BE%E0%A6%B2-%E0%A6%95%E0%A6%AE%E0%A6%BE%E0%A6%B0%E0%A7%8D%E0%A6%B8-%E0%A6%A8%E0%A7%80%E0%A6%A4%E0%A6%BF%E0%A6%AE%E0%A6%BE%E0%A6%B2%E0%A6%BE-%E0%A7%A8%E0%A7%A6%E0%A7%A7%E0%A7%AE (accessed 10 October 2022).

Mitchell, R.D. (2022), "What are the elements of common law fraud?", available at: www.robertdmitchell.com/common-law-fraud (accessed, 14 October 2022).

Montague, D. (2011), *Essentials of Online Payment Security and Fraud Prevention*, John Wiley and Sons, NJ.

Office of the Controller of Certifying Authorities (2022), "List of cas", available at: www.cca.gov.bd/site/page/a58193fd-99b7-45ea-b9ce-8df231598985/%E0%A6%B8%E0%A6%BF%E0%A6%8F%E0%A6%B8%E0%A6%AE%E0%A7%82%E0%A6%B9%E0%A7%87%E0%A6%B0-%E0%A6%A4%E0%A6%BE%E0%A6%B2%E0%A6%BF%E0%A6%95%E0%A6%BE (accessed 18 October 2022).

Sarkar, A. (2022a), "E-commerce scams: find out those responsible: HC", *The Daily Star*, 24 May, available at: www.thedailystar.net/news/bangladesh/news/find-out-those-responsible-hc-3030266 (accessed 24 November 2022).

Sarkar, A. (2022b), "Three online shops: BFIU finds evidence of money laundering", *The Daily Star*, 22 April, available at: www.thedailystar.net/news/bangladesh/crime-justice/news/three-online-shops-bfiu-finds-evidence-money-laundering-3009711 (accessed 7 November 2022).

Srivastava, A. (2011), "Resistance to change: six reasons why businesses don't use e-signatures", *Electronic Commerce Research*, Vol. 11 No. 4, pp. 357-382, doi: 10.1007/s10660-011-9082-4.

The Daily Star (2021a), "E-commerce firms must pay back their customers", 18 October, available at: www.thedailystar.net/views/editorial/news/e-commerce-firms-must-pay-back-their-customers-2200631 (accessed 6 October 2022).

The Daily Star (2021b), "Fraudulent practices in e-commerce cannot be tolerated, policy to protect customers, vendors must be introduced", 16 August, available at: www.thedailystar.net/views/editorial/news/fraudulent-practices-e-commerce-cannot-be-tolerated-2152971 (accessed 6 October 2022).

The Daily Star (2022), "5 Held for making fake NID, driving licence: Rab", 23 March, available at: www.thedailystar.net/news/bangladesh/news/5-held-making-fake-nid-driving-licence-rab-2988486 (accessed 18 October 2022).

The Digital Security Act (2018).

The New Age (2020), "KSA wants Bangladesh to issue passports to 54,000 Rohingyas: FM', 23 september", available at: www.newagebd.net/article/117077/ksa-wants-bangladesh-to-issue-passports-to-54000-rohingyas-fm (accessed, 18 October 2022).

The Sale of Goods Act (1930).

TIB (2020), "Corruption perceptions index", https://images.transparencycdn.org/images/CPI2020_Report_EN_0802-WEB-1_2021-02-08-103053.pdf (accessed 4 November 2022).

Uddin, A.Z. and Hasan, M. (2022), "Scams in 25 e-commerce firms, Ponzi schemes brought them Tk 6,050cr in just 4 months", *The Daily Star*, 17 March, available at: www.thedailystar.net/business/economy/news/ponzi-schemes-brought-them-tk-6050cr-just-4-months-2984746 (accessed 10 October 2022).

Uniform Electronic Transactions Act (UETA) (1999).

Vagadia, B. (2020), *Digital Disruption: Implications and Opportunities for Economies, Society, Policy Makers and Business Leaders*, Springer Nature, London.

Further reading

Bangladesh Electronic Funds Transfer Network (BEFTN) Operating Rules (2010).

BLAU v. America's servicing company (2009), No. CV-08-773-PHX-MHM (D. Ariz. Sep. 28, 2009).

Estate of Schwarz v. Philip Morris (2006), Inc., 206 Or. App. 20, 39, 135 P.3d 409, 422 (Or. Ct. App. 2006).
Markman v. Westview Instruments, Inc (1996), 517 U.S. 370.
Penal Code (1860).
Prudential Ins. Co. of America v. Anaya (1967), 78 N.M. 101, 104, 428 P.2d 640, 643.
Spinks v. Clark 147 Cal. 439, 82 P. 45 (Cal. 1905).
St. Louis S. F. R. Co. v. Reed (1913), 37 Okla. 350, 132 P. 355 (Okla. 1913)
Stokes v. Victory Land Co (1930), 99 Fla. 795, 802, 128 So. 408, 410.

Corresponding author
Md. Zahurul Haq can be contacted at: zahurul.haq@gmail.com

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**