

Lessons from London and Singapore: Rebuilding Malaysia's Shield against E-Commerce Fraud

Mohd Ardi Shah Bin Abd Rahman Shah

Faculty of Law, Universiti Teknologi MARA, Malaysia

DOI: <https://doi.org/10.47772/IJRISS.2026.100800894>

Received: 09 September 2026; Accepted: 14 September 2026; Published: 19 September 2026

ABSTRACT

The rapid expansion of e-commerce in Malaysia has significantly increased the incidence of fraudulent transactions, including non-delivery of goods, misleading product descriptions, counterfeit items, and sophisticated online scams. Despite the existence of key legislation such as the Consumer Protection Act 1999, the Electronic Commerce Act 2006, and the Consumer Protection (Electronic Trade Transaction) Regulations 2024, notable regulatory gaps remain in addressing platform liability, cross-border enforcement, seller verification, and effective consumer redress mechanisms. This article critically examines the adequacy of Malaysia's current legal framework in protecting consumers against e-commerce fraud. Through a comparative analysis with the United Kingdom (particularly the Digital Markets, Competition and Consumers Act 2024 and related consumer protection regimes) and Singapore (primarily the Consumer Protection (Fair Trading) Act and complementary anti-scam measures and industry guidelines), the study identifies strengths and weaknesses across the three jurisdictions. The findings reveal that while Malaysia has made progressive updates through recent regulations, it lags behind the United Kingdom's stronger direct enforcement powers and Singapore's more proactive platform accountability and anti-scam frameworks. Drawing on these comparative insights, the article proposes targeted legal reforms, enhanced institutional coordination, clearer platform liability rules, and improved dispute resolution mechanisms to strengthen Malaysia's e-commerce consumer protection regime and foster greater trust in the digital marketplace.

Keywords: Consumer protection, fraudulent transactions, Malaysia, Singapore, United Kingdom

INTRODUCTION

As evaluated by Mordor Intelligence (2026), the exponential growth of e-commerce has transformed Malaysia's retail landscape, offering consumers unprecedented convenience, wider product choices, and access to both domestic and international markets. Supported by high internet penetration, widespread smartphone usage, and government initiatives under the National E-Commerce Strategic Roadmap, Malaysia's e-commerce sector continues to expand rapidly and contributes significantly to the digital economy (Mordor Intelligence 2026). However, this digital transformation has been accompanied by a parallel surge in fraudulent transactions. Common forms of e-commerce fraud include non-delivery of goods, receipt of products that differ substantially from their online descriptions, the sale of counterfeit items, misleading pricing, and increasingly sophisticated scams conducted through online marketplaces and social commerce platforms (Cheong & Ahmad, 2023).

Official statistics reveal the severity of the problem (New Straits Times, 2026). According to the Minister of Domestic Trade and Cost of Living in a parliamentary reply, a total of 33,400 online fraud complaints were lodged between 2023 and 2025 (Armizan, 2026). According to figures reported by The Edge Malaysia citing statements by the Minister of Domestic Trade and Cost of Living, e-commerce-related scam losses exceeded RM430 million in the first three months of 2026 (The Edge Malaysia, 2026).

Malaysia's primary legal instruments governing consumer protection in electronic transactions include the Consumer Protection Act 1999 (as amended), the Electronic Commerce Act 2006, and the Consumer Protection (Electronic Trade Transaction) Regulations 2024. While these laws provide a foundational framework particularly through mandatory disclosure requirements and general prohibitions against unfair trade practices,

significant gaps persist. These include limited platform liability for third-party sellers, challenges in cross-border enforcement, insufficient mechanisms for rapid consumer redress, and difficulties in addressing emerging fraud tactics enabled by technology.

The objectives of this study are threefold: first, to critically evaluate the strengths and limitations of Malaysia's existing legal framework in combating e-commerce fraud; second, to identify transferable best practices from the United Kingdom and Singapore; and third, to propose concrete legal and policy reforms aimed at strengthening consumer protection, enhancing enforcement effectiveness, and restoring trust in Malaysia's digital marketplace.

The United Kingdom and Singapore were selected as comparative jurisdictions for both doctrinal and practical reasons. The United Kingdom was chosen because the Digital Markets, Competition and Consumers Act 2024 constitutes one of the most recent and comprehensive modernisations of consumer-protection enforcement in a common law jurisdiction with highly developed digital markets. It introduces expanded prohibitions on unfair commercial practices, including fake reviews and drip pricing together with powerful direct administrative enforcement powers for the Competition and Markets Authority. Singapore was selected as an ASEAN peer jurisdiction that shares a common-law legal tradition, a mature digital economy, and a hybrid regulatory model combining the Consumer Protection (Fair Trading) Act with industry codes of practice and strong inter-agency coordination. Official data indicate that this model has contributed to a measurable reduction in reported e-commerce scam cases. Together, the two jurisdictions therefore provide relevant, contemporary benchmarks against which Malaysia's framework can be evaluated and from which transferable lessons can be drawn.

LITERATURE REVIEW

Existing scholarship on Malaysian e-commerce consumer protection consistently identifies fragmentation and gaps in the Consumer Protection Act 1999 and the Electronic Commerce Act 2006 framework. Razali, Wan Rosli, and Othman (2022) document the inadequacy of existing Malaysian laws in addressing e-commerce fraud, while Sarabdeen (2025) empirically confirms persistent gaps in e-consumer protection. Zeno (2022) further highlights the need to reform information disclosure obligations in consumer contracts, noting that Malaysian law has not kept pace with digital marketplace developments. Cheong and Ahmad (2023) demonstrate that fraudulent transactions including non-delivery, counterfeit goods, and misleading descriptions continue to proliferate despite existing legislative instruments.

The United Kingdom's consumer protection framework has attracted significant scholarly attention following the enactment of the Digital Markets, Competition and Consumers Act 2024. Subagyo et al. (2025) observe that robust platform accountability and direct enforcement powers characterise the UK's evolving approach to digital consumer protection. Singapore's framework, anchored by the Consumer Protection (Fair Trading) Act and complemented by industry-driven anti-scam codes, is noted in comparative studies as a model of proactive platform governance particularly relevant for ASEAN jurisdictions (Tseng, 2023).

Despite a growing body of regional scholarship, there remains a notable absence of sustained comparative legal analysis between Malaysia, the United Kingdom, and Singapore that specifically addresses platform liability rules, seller verification obligations, cross-border enforcement, and consumer redress mechanisms in the context of e-commerce fraud. Tseng (2023) identifies ASEAN-wide harmonisation as an unresolved challenge, while existing Malaysian-focused studies do not systematically engage with the UK's Digital Markets, Competition and Consumers Act 2024 as a comparative benchmark. This article addresses that gap by conducting a structured comparative analysis to derive targeted reform recommendations for Malaysia.

METHODOLOGY

This study adopts a doctrinal and comparative legal research approach. The doctrinal method involves a systematic examination, interpretation, and critical analysis of primary legal sources to determine the current state of the law and identify its strengths and shortcomings in addressing e-commerce fraud. The comparative method is employed to evaluate Malaysia's legal framework against selected foreign jurisdictions with more mature or progressive regulatory responses to similar challenges.

Research Design

The research is qualitative and analytical in nature. It focuses on the substantive content, scope, and practical effectiveness of legal provisions governing consumer protection in electronic commerce, with particular emphasis on fraudulent transactions (including non-delivery, misleading representations, counterfeit goods, and platform-related misconduct).

Primary Sources

The primary legal materials examined include:

Malaysia

- Consumer Protection Act 1999 (Act 599), particularly Parts II (Misleading and Deceptive Conduct), IIIA (Unfair Contract Terms), V (Guarantees in Respect of Supply of Goods), and related enforcement provisions;
- Consumer Protection (Electronic Trade Transaction) Regulations 2024;
- Electronic Commerce Act 2006 (Act 658); and
- Personal Data Protection Act 2010 (Act 709), insofar as it relates to the handling of consumer data in online transactions.

United Kingdom

- Digital Markets, Competition and Consumers Act 2024 (particularly the consumer protection and unfair trading provisions);
- Consumer Rights Act 2015;
- Consumer Protection from Unfair Trading Regulations 2008 (as amended and largely superseded); and
- Data Protection Act 2018.

Singapore

- Consumer Protection (Fair Trading) Act 2003;
- Electronic Transactions Act 2010; and
- Personal Data Protection Act 2012.

Secondary Sources

Secondary materials include peer-reviewed journal articles, official government reports and policy papers (particularly from the Ministry of Domestic Trade and Cost of Living, the Competition and Markets Authority, and Singapore's Competition and Consumer Commission), academic commentaries, and relevant industry guidelines on e-commerce platform accountability and anti-scam measures. These sources are used to contextualise the legal provisions, assess enforcement realities, and identify practical gaps that pure statutory analysis may not fully reveal.

Comparative Framework

The comparative analysis is structured around four key dimensions critical to e-commerce consumer protection against fraud:

1. Scope of prohibitions against misleading and unfair commercial practices;
2. Duties and liabilities of online marketplace operators and third-party sellers;
3. Information disclosure and transparency obligations; and
4. Enforcement mechanisms, remedies, and access to redress (including platform liability and alternative dispute resolution).

Scope and Limitations

The study is confined to consumer-to-business (B2C) electronic trade transactions and does not extend to business-to-business dealings or pure criminal fraud prosecuted under penal statutes. It focuses primarily on statutory and regulatory frameworks rather than an exhaustive survey of case law, given the relative scarcity of reported Malaysian decisions specifically addressing sophisticated e-commerce fraud. Cross-border enforcement challenges are discussed but not examined in full private international law detail. Comprehensive official longitudinal statistical series specifically disaggregating e-commerce fraud from broader online scam categories remain limited in Malaysia, accordingly, the most recent figures are drawn from parliamentary replies and official statements by the Ministry of Domestic Trade and Cost of Living, the Royal Malaysia Police, and the National Scam Response Centre, as reported in contemporary media where primary documents are not yet publicly archived.

Comparative Legal Frameworks

This section outlines the principal legal frameworks governing e-commerce consumer protection against fraudulent transactions in Malaysia, the United Kingdom, and Singapore. Contemporary digital consumer protection scholarship increasingly recognises that traditional bilateral models of trader–consumer regulation are inadequate in platform-mediated markets. Online marketplaces function as gatekeepers that structure information flows, ranking algorithms, payment systems, and dispute resolution pathways. Regulatory theory therefore shifts attention from pure ex-post liability toward a combination of ex-ante due-diligence obligations, co-regulatory instruments, and strong administrative enforcement capacity. This comparative adopts a pragmatic regulatory perspective that evaluates legal frameworks according to their capacity to induce preventive platform behaviour, enable rapid redress, and generate credible deterrence rather than solely according to the formal completeness of substantive rights. The analysis that follows is therefore conducted with full awareness of the contextual differences between the three jurisdictions.

While the United Kingdom and Singapore offer valuable comparative insights, important contextual differences limit the direct transferability of their approaches to Malaysia. Malaysia's e-commerce market is smaller and more fragmented than those of the United Kingdom or Singapore, with a greater prevalence of social-commerce and informal live-streaming channels alongside the major platforms. Institutionally, the Competition and Markets Authority in the United Kingdom possesses significantly greater resources, investigative capacity, and direct administrative penalty powers than the Ministry of Domestic Trade and Cost of Living or the Controller under the Consumer Protection Act 1999. Singapore benefits from a tightly coordinated inter-agency culture, high levels of industry buy-in, and a well-resourced operational anti-scam infrastructure that Malaysia's more siloed multi-agency structure has not yet fully replicated. Although all three jurisdictions share a common-law heritage that facilitates the borrowing of legal concepts, Malaysia currently lacks the statutory administrative-penalty regime of the United Kingdom and relies less heavily on soft-law instruments than Singapore. Consequently, the recommendations advanced in this article adapt rather than transplant the foreign models, focusing on a hybrid due-diligence standard for platforms and graduated administrative enforcement powers that can be realistically calibrated to Malaysia's institutional and market conditions.

Malaysia

Malaysia's framework is primarily anchored in the Consumer Protection Act 1999 (Act 599) ("CPA 1999"), supplemented by the Consumer Protection (Electronic Trade Transaction) Regulations 2024 ("2024

Regulations”), the Electronic Commerce Act 2006 (Act 658), and, to a limited extent, the Personal Data Protection Act 2010 (Act 709).

The CPA 1999 applies expressly to trade transactions conducted through electronic means (section 2). Part II prohibits misleading conduct (section 9), false or misleading representations (section 10), misleading indications as to price (section 12), bait advertising (section 13), and demanding or accepting payment without intending to supply (section 16). Part IIIA addresses unfair contract terms, while Parts V–IX provide implied guarantees as to acceptable quality, fitness for purpose, and compliance with description, together with consumer rights of redress against suppliers and manufacturers (Amin & Mohd Nor, 2013).

The 2024 Regulations (which came into force on 25 December 2024 and revoked the 2012 Regulations) introduce specific rules for online marketplaces. Key features include:

- a) Mandatory disclosure by online marketplace suppliers of detailed information (name, contact details, full price including all costs, main characteristics of goods/services, terms and conditions, estimated delivery time, and safety/health certifications) (Regulation 3 and Schedule);
- b) Prohibition on disclosing false or misleading information;
- c) Requirement that disclosures be made in the national language (Bahasa Malaysia), with other languages permitted as supplements;
- d) Duties on suppliers to bear re-delivery costs for materially different or defective goods and to provide reasonably fit services (Regulation 5);
- e) Obligations to enable error rectification and to acknowledge orders without undue delay (Regulation 6);
- f) Duties on online marketplace operators to ensure supplier compliance with disclosure rules before permitting transactions, to provide a complaints channel, and to prevent non-compliant advertising (Regulation 7); and
- g) Record-keeping obligations for three years (Regulation 8).

Non-compliance constitutes an offence under the Regulations and is enforceable under the CPA 1999. The Tribunal for Consumer Claims provides an accessible forum for claims (generally up to RM50,000 following amendments), while the Ministry of Domestic Trade and Cost of Living (KPDN) holds investigative and enforcement powers. Despite the improvements introduced by the 2024 Regulations, significant structural limitations remain, particularly in relation to platform liability, proactive monitoring duties, and cross-border enforcement. These weaknesses are examined in detail in Section 7, Critical Analysis And Challenges.

United Kingdom

The United Kingdom’s regime has been substantially modernised by the Digital Markets, Competition and Consumers Act 2024 (“DMCC Act 2024”), which largely replaces and strengthens the Consumer Protection from Unfair Trading Regulations 2008 (“CPUTR 2008”). It operates alongside the Consumer Rights Act 2015 (“CRA 2015”) and the Data Protection Act 2018. The DMCC Act 2024 represents a structural redesign of UK consumer enforcement rather than a mere updating of substantive rules. Part 4, Chapter 1 restates the general prohibition on unfair commercial practices and significantly expands the blacklist of practices that are unfair in all circumstances.

Two expansions are particularly relevant to e-commerce fraud. First, the Act expressly prohibits the submitting or commissioning of fake consumer reviews, as well as the failure by a trader to take reasonable and proportionate steps to prevent the publication of such reviews. This moves beyond the previous, more general prohibition on misleading commercial practices and creates a specific, platform-relevant duty. Second, the Act targets “drip pricing” by prohibiting the presentation of a price that omits mandatory charges or fees that the consumer will necessarily have to pay, where those charges are only revealed later in the purchasing process.

Both practices are now classified as unfair in all circumstances, removing the need for the enforcement authority to prove that they would be likely to distort the economic behaviour of the average consumer.

These substantive expansions are deliberately paired with the new administrative enforcement architecture in Part 3. Under Part 3, the Competition and Markets Authority may investigate suspected infringements, impose financial penalties of up to 10 per cent of global turnover, order consumer redress, and issue enforcement notices without first obtaining a court order. The relationship between Part 3 and Part 4 is therefore symbiotic: the expanded blacklist in Part 4 supplies clear and specific legal bases for intervention, while the direct administrative powers in Part 3 supply the speed and deterrent force that were lacking under the previous court-dependent model of the Consumer Protection from Unfair Trading Regulations 2008. The UK's combination of expanded substantive prohibitions and direct administrative enforcement powers provides a useful benchmark for assessing the relative weakness of Malaysia's current enforcement architecture, a comparison that is developed more fully in Section 7, Critical Analysis And Challenges.

Singapore

Singapore's primary instrument is the Consumer Protection (Fair Trading) Act 2003 ("CPFTA"), administered by the Competition and Consumer Commission of Singapore (CCCS). It is complemented by the Electronic Transactions Act 2010 and the Personal Data Protection Act 2012, together with industry guidelines such as Technical Reference 76 (TR 76) on electronic commerce transactions and enhanced anti-scam codes of practice under the Online Criminal Harms Act 2023. Singapore's consumer protection framework in the e-commerce context is best understood as a hybrid system that combines a relatively broad statutory prohibition on unfair practices under the Consumer Protection (Fair Trading) Act 2003 with extensive reliance on soft-law instruments, voluntary compliance, and operational coordination.

The CPFTA itself does not impose detailed, prescriptive duties on online marketplace operators equivalent to those found in Malaysia's 2024 Regulations. Instead, much of the practical burden of prevention is carried by codes of practice issued under the Online Criminal Harms Act 2023, Technical Reference 76, the E-commerce Marketplace Transaction Safety Ratings system, and voluntary undertakings negotiated by the Competition and Consumer Commission of Singapore.

Publicly available materials indicate that the codes of practice applicable to designated e-commerce services typically require platforms to:

- (a) implement systems capable of detecting and disrupting scam activity on an ongoing basis (including both automated tools and human review);
- (b) conduct appropriate verification of sellers before allowing them to list goods or services;
- (c) retain relevant transactional and user data for a prescribed period to facilitate investigation;
- (d) respond to directions from the relevant authorities within short, specified timeframes (commonly measured in hours rather than days); and
- (e) maintain channels for rapid user reporting and inter-agency information sharing.

These obligations go beyond traditional notice-and-takedown duties and create a form of continuous, technology-enabled due diligence. Compliance is further incentivised by reputational mechanisms such as the E-commerce Marketplace Transaction Safety Ratings and by the possibility of regulatory directions or further statutory measures in the event of persistent non-cooperation.

This soft-law and coregulatory emphasis has advantages of flexibility and speed, but it also means that the formal legal obligations on platforms remain less prescriptive and less judicially enforceable than a pure statutory duty of care. Effectiveness depends heavily on the willingness of major platforms to cooperate, the credibility of reputational incentives, and the operational capacity of agencies such as the Singapore Police Force and the Online Criminal Harms Act Office. In other words, Singapore's comparatively strong outcomes appear to rest

as much on institutional culture, inter-agency coordination, and industry buy-in as on the formal strength of statutory text. Singapore's hybrid model, which relies heavily on soft-law instruments and operational coordination, offers important practical lessons. However, the transferability of this approach to Malaysia, and the continuing gaps in Malaysia's own framework, are critically assessed in Section 7, Critical Analysis And Challenges.

Preliminary Comparative Observations

Malaysia has made progress with the 2024 Regulations, particularly in disclosure duties. However, it still lacks the direct administrative enforcement powers of the UK CMA and the more developed platform accountability mechanisms seen in Singapore. These structural gaps are analysed in detail in Section 7, Critical Analysis And Challenges.

Institutional Mechanisms And Implementation

Effective consumer protection against e-commerce fraud depends not only on the substantive content of the law but also on the institutional architecture and practical implementation mechanisms that support enforcement, redress, and deterrence. This section examines the key institutional arrangements in Malaysia, the United Kingdom, and Singapore, focusing on regulatory bodies, enforcement powers, dispute resolution forums, and coordination mechanisms.

Malaysia

Malaysia's institutional framework for e-commerce consumer protection is multi-agency and primarily centred on the Ministry of Domestic Trade and Cost of Living (KPDN). Under the Consumer Protection Act 1999, the Minister appoints a Controller, Deputy Controllers, and Assistant Controllers who exercise investigative, enforcement, and compounding powers. KPDN is responsible for monitoring compliance with the Consumer Protection (Electronic Trade Transaction) Regulations 2024, handling consumer complaints, conducting investigations, and initiating prosecutions or administrative actions.

The Tribunal for Consumer Claims provides an accessible, low-cost forum for individual consumers to seek redress for claims arising from defective goods, non-delivery, or unfair practices (subject to jurisdictional monetary limits). The Tribunal emphasises speedy and informal resolution, with decisions that are generally final and binding (Mohd Mokhtar, 2025).

Other relevant bodies include:

- The Malaysian Communications and Multimedia Commission (MCMC), which addresses online content, scam advertisements, and platform-related issues under the Communications and Multimedia Act 1998 and the Online Safety Act;
- The National Scam Response Centre (NSRC), which coordinates rapid response to scam reports, including freezing of funds;
- The Royal Malaysia Police (Commercial Crime Investigation Department), which investigates criminal fraud; and
- The Personal Data Protection Department, which oversees data-related aspects of online transactions.

Despite these structures, implementation faces several challenges. Enforcement of the 2024 Regulations is still relatively new, coordination among agencies can be fragmented, platform operators' compliance monitoring remains largely reactive, and cross-border cases are difficult to pursue effectively. Consumer awareness of rights and available redress channels also varies.

United Kingdom

The DMCC Act 2024 marks a decisive shift in UK consumer enforcement. Under Part 3, the CMA may now impose financial penalties of up to 10% of a trader's global turnover and order consumer redress without first obtaining a court injunction. This power is complemented by an expanded blacklist of commercial practices that are unfair in all circumstances, including the publication of fake reviews and drip pricing. The combination of substantive expansion and direct administrative sanctions significantly increases both the speed and the deterrent effect of enforcement compared with the previous regime under the Consumer Protection from Unfair Trading Regulations 2008.

Local Trading Standards services continue to play an important role in frontline enforcement and consumer advice. Consumers also have access to private rights of action under the Consumer Rights Act 2015 and can utilise alternative dispute resolution schemes. The CMA prioritises systemic issues affecting large numbers of consumers, such as fake reviews, drip pricing, and unfair online practices by major platforms.

Implementation is characterised by proactive market monitoring, data-driven prioritisation of cases, public guidance, and high-profile enforcement actions that serve both punitive and deterrent functions. Inter-agency cooperation (including with the Information Commissioner's Office on data issues) further supports a coherent regulatory response.

Singapore

Singapore employs a dual approach combining statutory enforcement by the Competition and Consumer Commission of Singapore (CCCS) with practical, collaborative mechanisms involving industry and consumer bodies. Under the Consumer Protection (Fair Trading) Act 2003, CCCS has powers to investigate unfair practices, enter into voluntary compliance agreements with suppliers, and seek court declarations or injunctions. It can also take action against parties who abet or procure unfair practices.

The Consumers Association of Singapore (CASE) plays a significant complementary role through mediation, the CaseTrust accreditation scheme, and the promotion of the Standard Dispute Management Framework adopted by major e-commerce platforms. The Small Claims Tribunals provide an accessible judicial forum for lower-value consumer claims.

Under the codes of practice issued pursuant to the Online Criminal Harms Act 2023, designated e-commerce services are required to implement systems capable of proactively detecting scam activity, to retain relevant transactional data, and to respond to regulatory directions within short prescribed timeframes. These obligations go beyond traditional notice-and-takedown duties and create a form of continuous, technology-enabled due diligence. Empirical reports suggest that the combination of these platform-level duties with operational coordination has contributed to a measurable decline in reported e-commerce scam cases, although attribution remains complex. The Singapore Police Force and the Online Criminal Harms Act Office oversee compliance, while the Monetary Authority of Singapore addresses payment-related protections. Technical Reference 76 and the E-commerce Marketplace Transaction Safety Ratings further encourage platforms to adopt robust seller verification, payment protection, and dispute resolution measures.

Implementation in Singapore emphasises rapid response, industry co-regulation, public education, and measurable platform accountability (for example through safety ratings). This multi-layered model has contributed to noticeable reductions in certain categories of e-commerce scams.

Comparative Assessment of Institutional Effectiveness

The three jurisdictions reveal distinct institutional philosophies. Malaysia relies on a traditional ministry-led model with a specialised consumer tribunal, which offers accessibility for individual claims but currently lacks the strong, centralised administrative enforcement powers seen in the United Kingdom. The UK's post-2024 CMA regime prioritises high-impact, systemic enforcement with significant deterrent capacity. Singapore combines statutory powers with extensive soft-law instruments, industry collaboration, and specialised anti-

scam infrastructure, producing a pragmatic and relatively agile system. The comparative institutional analysis reveals clear differences in enforcement capacity and platform accountability. The implications of these differences for Malaysia, and the reforms needed to address them, are considered in Section 7, Critical Analysis And Challenges.

Effectiveness And Empirical Evidence

While the existence of legal frameworks and institutional mechanisms is a necessary foundation, their real-world effectiveness must be assessed through empirical indicators such as complaint volumes, financial losses, enforcement outcomes, consumer recovery rates, and observable changes in market behaviour. This section evaluates the practical performance of the regimes in Malaysia, the United Kingdom, and Singapore, drawing on available official statistics, enforcement reports, and secondary data.

Malaysia

Empirical evidence indicates that Malaysia continues to face significant challenges in curbing e-commerce fraud despite recent legislative updates. Between 2023 and 2025, more than 33,400 complaints related to online fraud were lodged, forming a substantial portion of the over 136,000 commercial transaction complaints received by the Ministry of Domestic Trade and Cost of Living (KPDN) (Armizan, 2026). Online transactions consistently rank as the highest category of consumer complaints, with common issues including non-receipt of goods or services, discrepancies between advertised and delivered items, misleading pricing, and counterfeit products (The Star, 2026).

Overall online scam losses reached RM2.97 billion in 2025 (Mohd Khalid, 2026). In the first quarter of 2026, e-commerce fraud cases reportedly surged by around 92% compared with the same period in the previous year (The Vibes, 2026). Enforcement activity includes compounds, prosecutions under the Consumer Protection Act 1999, website blocking, and content removal actions (thousands of blocks and removals recorded between 2021 and 2025). However, the number of successful court prosecutions specifically under consumer protection provisions remains relatively modest, and recovery of losses for individual victims is often limited (New Straits Times, 2026).

The Consumer Protection (Electronic Trade Transaction) Regulations 2024 represent a positive step by clarifying disclosure duties and operator responsibilities. Yet, given their recent entry into force (25 December 2024), comprehensive empirical data on their impact is still emerging. Early indications suggest improved formal compliance by major platforms, but sophisticated fraud tactics, cross-border sellers, and social-commerce channels continue to pose enforcement difficulties. Overall, the data point to a persistent gap between the formal legal framework and effective deterrence or victim redress.

United Kingdom

The United Kingdom's post-2024 regime under the Digital Markets, Competition and Consumers Act 2024 has begun to demonstrate tangible enforcement effects. The Competition and Markets Authority (CMA) has utilised its new direct administrative powers to launch multiple investigations into online pricing practices, drip pricing, and unfair commercial conduct. In one early high-profile case, the CMA imposed a £4.2 million fine and ordered over £760,000 in customer refunds against driving-school operators for unlawful drip-pricing practices: CMA v AA Driving School and BSM Driving School (2026), a case involving more than 80,000 affected customers decided within five months of the DMCC Act 2024 enforcement powers coming into force in April 2025 (Competition and Markets Authority, 2026).

The CMA has prioritised systemic online harms, including fake reviews and hidden fees, issuing numerous advisory and warning letters alongside formal investigations. These interventions signal a shift toward faster, more deterrent enforcement compared with the previous court-reliant model. While comprehensive longitudinal data on overall reductions in e-commerce fraud are still developing, the combination of substantial financial penalties, mandatory redress, and public guidance appears to be increasing compliance pressure on large traders

and platforms. Consumer confidence metrics and complaint trends will require longer-term monitoring, but early enforcement outcomes suggest improved institutional effectiveness.

Singapore

Singapore provides comparatively stronger evidence of positive impact from coordinated legal, institutional, and industry measures. Official data indicate that e-commerce scams more than halved in certain recent periods. Official data from the Singapore Police Force show that e-commerce scam cases fell from 7,224 in the first half of 2024 to 3,237 in the first half of 2025 (Singapore Police Force, 2025). Official data indicate a substantial reduction in reported e-commerce scam cases between the first half of 2024 and the first half of 2025. While multiple factors are likely to have contributed including enhanced platform codes of practice, seller verification measures, public education campaigns, and improved inter-agency coordination on the temporal correlation with the introduction of stronger platform obligations under the Online Criminal Harms Act framework is noteworthy.

The E-commerce Marketplace Transaction Safety Ratings system, published annually by the Inter-Ministry Committee on Scams, and the enhanced Technical Reference 76 (TR 76) guidelines have incentivised major platforms to implement stronger seller verification, monitoring and remediation measures (Inter-Ministry Committee on Scams, 2024; Ministry of Home Affairs, 2025). CCCS enforcement through voluntary compliance agreements, investigations, and injunctions, combined with accessible Small Claims Tribunal (SCT) processes and Consumers Association of Singapore (CASE) mediation, contributes to relatively efficient dispute resolution. While absolute elimination of fraud remains impossible, the measurable reduction in reported e-commerce scam cases and associated losses demonstrates the effectiveness of a multi-layered approach that integrates statutory powers, soft-law instruments, platform duties, and inter-agency coordination.

Comparative Synthesis

Empirical patterns reveal clear differences in effectiveness. Malaysia continues to record high and, in some periods, rising volumes of e-commerce fraud complaints and substantial financial losses, indicating that existing legal and institutional tools have not yet achieved strong deterrent or protective outcomes. The United Kingdom is in the early stages of leveraging powerful new administrative enforcement capabilities, with promising initial cases that prioritise systemic harms. Available official statistics suggest that Singapore has achieved a more pronounced reduction in reported e-commerce scam cases than Malaysia during the same period. Caution is nevertheless required in drawing direct causal inferences, given differences in market size, reporting practices, and the concurrent operation of multiple policy interventions.

These findings underscore that legislative provisions alone are insufficient. Effectiveness depends heavily on the strength of enforcement powers, the clarity and enforceability of platform obligations, the speed of inter-agency coordination, the accessibility of redress, and the ability to adapt to evolving fraud techniques. The comparative evidence supports the case for targeted reforms in Malaysia that draw on the more robust enforcement model of the United Kingdom and the practical, results-oriented platform accountability measures observed in Singapore.

Critical Analysis And Challenges

Despite progressive legislative developments, particularly the enactment of the Consumer Protection (Electronic Trade Transaction) Regulations 2024, Malaysia's e-commerce consumer protection framework continues to exhibit significant structural and operational weaknesses when measured against the more robust regimes of the United Kingdom and Singapore. This section critically analyses the principal deficiencies of the Malaysian framework and identifies the key challenges that impede effective protection against fraudulent transactions.

Limitations of the Substantive Legal Framework

The Consumer Protection Act 1999 provides a solid general foundation through its prohibitions on misleading conduct, false representations, and unfair contract terms, as well as implied guarantees of quality and fitness (Zeno, 2022). The 2024 Regulations represent a meaningful advance by imposing specific disclosure obligations

on online marketplace suppliers and limited duties on operators, including ensuring supplier compliance, providing complaint channels, and maintaining records. However, several critical gaps remain.

First, platform liability is underdeveloped. Online marketplace operators are required to take reasonable steps to ensure disclosure compliance and to provide complaint mechanisms, but they are not subject to clear statutory duties of due diligence regarding seller verification, proactive monitoring of fraudulent listings, or secondary liability for third-party misconduct (Razali et al., 2022; Abdul Manap et al., 2022). In contrast, the United Kingdom's post-2024 regime under the Digital Markets, Competition and Consumers Act places stronger expectations on traders and platforms concerning fake reviews and unfair practices, while Singapore's combination of unfair practice rules and anti-scam codes of practice effectively pressures platforms to implement robust preventive controls. The United Kingdom's Digital Markets, Competition and Consumers Act 2024, which imposes explicit duties on platforms regarding fake reviews and unfair commercial practices, provides direct comparative authority for the introduction of analogous statutory due-diligence and secondary-liability obligations on Malaysian platform operators.

Second, the framework remains largely reactive. Liability is generally triggered after harm has occurred, with limited proactive obligations on platforms to detect and disrupt fraud in real time. Singapore's codes of practice under the Online Criminal Harms Act, which require designated e-commerce services to proactively detect scam activity and respond rapidly to regulatory requests, offer a more preventive model.

Third, cross-border enforcement and jurisdiction present persistent difficulties. Many fraudulent sellers operate from outside Malaysia, rendering traditional enforcement mechanisms under the Consumer Protection Act 1999 and the Tribunal for Consumer Claims of limited practical utility. Neither the Malaysian nor the comparator frameworks fully solve the private international law challenges of online fraud, but Singapore's emphasis on platform-level controls and the United Kingdom's stronger domestic enforcement create greater practical deterrence within their territories.

Cross-Border Enforcement Challenges

Cross-border e-commerce fraud presents one of the most intractable problems for the Malaysian framework. Many fraudulent sellers operate from outside Malaysia, frequently using foreign payment intermediaries, drop-shipping arrangements, or temporary online storefronts. In such cases, the conventional enforcement tools of the Consumer Protection Act 1999 and the Tribunal for Consumer Claims where investigation, compounding, prosecution, and tribunal awards encounter significant jurisdictional and practical obstacles.

From a private international law perspective, difficulties arise at multiple stages. Establishing jurisdiction over a foreign seller, serving process, obtaining evidence, and enforcing a Malaysian tribunal award or court judgment abroad are often costly and uncertain. Even where a consumer succeeds in obtaining an award, recovery is frequently impossible once the seller has disappeared or holds no assets within Malaysia. The 2024 Regulations do not materially improve this position, as their obligations are directed primarily at local or locally accessible operators and suppliers.

In practice, online platforms have become the most realistic enforcement nodes. Because major marketplaces control access to the Malaysian consumer market, payment flows, and seller accounts, they are often better placed than national authorities to freeze funds, remove listings, suspend sellers, or facilitate refunds. Both the United Kingdom and Singapore have, to varying degrees, recognised this reality by placing greater preventive and responsive duties on platforms, thereby converting them into *de facto* gatekeepers for cross-border consumer protection. Malaysia's current limited platform liability model does not fully exploit this potential.

Regional solutions remain under-developed. Although ASEAN has discussed e-commerce cooperation and consumer protection, there is as yet no robust mutual recognition or mutual assistance framework that would enable Malaysian authorities to obtain meaningful cooperation from counterparts in key source countries of fraudulent goods. Until such mechanisms mature, the most effective short- to medium-term strategy is to strengthen the obligations of platforms that intermediate cross-border sales into Malaysia, requiring them to

verify foreign sellers, maintain local points of contact, and assist in the execution of consumer remedies where reasonably practicable.

In short, while neither Malaysia nor its comparator jurisdictions have fully solved the private international law challenges of online fraud, a platform-centred approach offers a more practical route to mitigation than reliance on traditional cross-border judicial processes alone.

Platform Liability Analysis

A central deficiency in the Malaysian framework is the absence of a coherent statutory model of platform liability. Four principal models can be distinguished.

First, a pure notice-and-takedown (safe-harbour) model immunises the platform until it has actual knowledge of specific unlawful content and fails to act. This model prioritises platform innovation but is poorly suited to fast-moving e-commerce fraud, where the seller frequently disappears before a notice can be processed.

Second, a knowledge-based model imposes liability where the platform knew or ought reasonably to have known of the fraudulent activity. While more flexible, it generates uncertainty and high litigation costs.

Third, a due-diligence or “duty of care” model requires platforms to implement reasonable preventive systems including seller verification (KYC), automated and human monitoring of listings, and rapid removal protocols regardless of specific notice. This is the approach reflected in Singapore’s codes of practice under the Online Criminal Harms Act 2023 and, in more detailed form, in the EU Digital Services Act 2022 (which does not apply in the United Kingdom).

Fourth, a strict or secondary liability model would render the platform jointly and severally liable with the seller for consumer losses arising from non-delivery or counterfeit goods. While highly protective of consumers, such a model risks over-deterrence and is politically and economically challenging in a developing digital market.

For Malaysia, a hybrid due-diligence model is the most appropriate. It should combine: (a) mandatory pre-listing seller verification; (b) an obligation to maintain reasonable systems for detecting and removing fraudulent listings; and (c) accelerated liability once the platform has actual knowledge and fails to act within a prescribed short period (e.g., 24–48 hours). This model draws on Singapore’s practical experience while remaining more proportionate than strict liability. It can be introduced by amending Regulation 7 of the 2024 Regulations and inserting a new dedicated section on platform duties in the Consumer Protection Act 1999.

Institutional and Enforcement Challenges

Institutionally, Malaysia’s multi-agency structure centred on the Ministry of Domestic Trade and Cost of Living, supported by the Tribunal for Consumer Claims, MCMC, the National Scam Response Centre, and the police suffers from coordination fragmentation. Overlapping mandates can lead to delayed responses, inconsistent prioritisation, and difficulties in pursuing complex, technology-enabled fraud cases.

Enforcement powers remain comparatively weak. Unlike the United Kingdom’s Competition and Markets Authority, which now possesses direct administrative powers to impose substantial fines (up to 10% of global turnover) and order consumer redress without prior court approval, Malaysian authorities largely rely on investigation, compounding, prosecution, and tribunal adjudication. This court- or tribunal-dependent model is slower and less deterrent against large or sophisticated operators. Empirical evidence of high and rising complaint volumes, substantial financial losses, and relatively modest prosecution numbers underscores the limited deterrent effect of the current system.

Access to effective redress is another concern. Although the Tribunal for Consumer Claims offers an accessible forum, recovery rates for victims of sophisticated e-commerce fraud especially involving non-delivery by overseas sellers or vanished platforms are often low. Consumers face evidentiary burdens, jurisdictional hurdles, and practical difficulties in enforcing awards.

Technological and Market Evolution Challenges

The rapid evolution of e-commerce business models poses further difficulties. Social commerce, live-streaming sales, and peer-to-peer transactions on messaging platforms frequently fall into regulatory grey areas. Fraudsters continually adapt tactics, including the use of deepfakes, fake reviews, and sophisticated phishing, outpacing static legal provisions. While the 2024 Regulations improve transparency, they do not adequately address algorithmic ranking opacity, dark patterns, or the responsibilities of platforms in moderating user-generated commercial content.

Data protection dimensions under the Personal Data Protection Act 2010 are only loosely integrated with consumer protection enforcement, limiting the ability to address fraud that exploits personal data or involves identity misuse.

Social Commerce and Live-Streaming Sales

A particularly acute regulatory gap concerns social commerce and live-streaming sales. These business models in which sellers promote and conclude transactions through social media platforms, messaging applications, or live-stream sessions have expanded rapidly in Malaysia. They often blur the distinction between private communication and commercial activity and frequently involve informal or unverified sellers who do not operate through established online marketplaces.

The Consumer Protection (Electronic Trade Transaction) Regulations 2024 are primarily designed for structured online marketplaces. Their disclosure obligations, operator duties, and record-keeping requirements apply most clearly to platforms that systematically facilitate transactions between multiple sellers and buyers. Social commerce and live-streaming arrangements frequently fall outside this structured model. Sellers may operate through personal accounts, temporary live sessions, or closed messaging groups, making it difficult to identify the “online marketplace operator” upon whom Regulation 7 duties can be imposed. In many cases there is no clear intermediary that can be required to conduct seller verification, maintain complaint channels, or retain transaction records.

This regulatory ambiguity creates a significant enforcement vacuum. Consumers who purchase goods through live-streams or social media often face heightened risks of non-delivery, counterfeit products, and disappearing sellers, yet they may struggle to invoke the specific protections of the 2024 Regulations. While the general prohibitions in Part II of the Consumer Protection Act 1999 (misleading conduct, false representations, and demanding payment without intention to supply) remain applicable, the absence of tailored disclosure and platform duties reduces both preventive effect and practical redress.

Comparative experience suggests that leaving social commerce largely unregulated is unsustainable. Singapore has begun to extend anti-scam expectations and platform accountability measures to a wider range of online services, while the United Kingdom’s expanded unfair-trading rules under the DMCC Act 2024 are capable of reaching misleading practices regardless of the technical medium. Malaysia will need to consider either expanding the definition of “online marketplace operator” or introducing specific obligations for social media and messaging platforms that systematically facilitate commercial transactions. Without such adaptation, a growing segment of e-commerce activity will remain only partially covered by the current framework.

Comparative Insights and Systemic Assessment

Comparative analysis reveals that the United Kingdom has prioritised institutional empowerment and high-impact administrative enforcement, enabling faster responses to systemic online harms. Singapore has achieved measurable reductions in e-commerce scam incidence through a pragmatic blend of statutory unfair practice rules, detailed platform codes of practice, seller verification expectations, and strong inter-agency operational coordination. Malaysia’s framework, while improved in formal disclosure requirements, remains closer to a traditional, reactive consumer protection model that has not kept pace with the scale and sophistication of digital fraud. The core challenge is therefore not the complete absence of legal tools, but the insufficiency of those tools

in scope, enforceability, platform accountability, and institutional capacity. Without addressing these structural weaknesses, legislative updates risk remaining symbolic rather than transformative.

RECOMMENDATIONS FOR MALAYSIA

Drawing on the comparative analysis of the legal frameworks, institutional mechanisms, and empirical outcomes in the United Kingdom and Singapore, this section proposes targeted recommendations to strengthen Malaysia's e-commerce consumer protection regime against fraudulent transactions. The recommendations aim to address the identified gaps in platform accountability, enforcement capacity, preventive measures, and consumer redress while remaining sensitive to Malaysia's legal and institutional context.

Strengthen Statutory Duties and Liability of Online Marketplace Operators

It is recommended that Regulation 7 of the Consumer Protection (Electronic Trade Transaction) Regulations 2024 be amended to impose the following additional duties on online marketplace operators: (a) mandatory verification of the identity and contact details of all third-party sellers before listings are permitted; (b) an obligation to implement and maintain reasonable systems (including both automated tools and human review) for the detection and prompt removal of listings that are false, misleading, or indicative of non-delivery risk; and (c) secondary liability for consumer losses arising from non-delivery or counterfeit goods where the operator has received actual notice of the problem and fails to take reasonable steps to prevent further transactions or to facilitate redress within 48 hours. Concurrently, a new section should be inserted into Part II of the Consumer Protection Act 1999 creating a statutory duty of care on online marketplace operators in respect of third-party sellers.

Enhance Administrative Enforcement Powers

The Consumer Protection Act 1999 should be amended to confer on the Controller (or a designated senior officer) the power to: (a) issue binding compliance notices; (b) impose administrative financial penalties of up to a prescribed percentage of the trader's annual turnover in Malaysia (or a fixed maximum, whichever is higher); and (c) order the payment of consumer redress in cases involving systemic or widespread harm, without the necessity of first commencing proceedings in court or the Tribunal. These powers should be modelled, with appropriate adaptations, on the direct enforcement powers conferred on the UK Competition and Markets Authority under Part 3 of the Digital Markets, Competition and Consumers Act 2024.

Establish a Coordinated National E-Commerce Consumer Protection Mechanism

A National E-Commerce Consumer Protection Coordinating Committee should be established by ministerial order, comprising senior representatives of KPDN, MCMC, the National Scam Response Centre, the Royal Malaysia Police (Commercial Crime Investigation Department), and the Personal Data Protection Department. The Committee should be mandated to meet at least quarterly, to share real-time intelligence on emerging fraud patterns, and to develop joint standard operating procedures for high-impact cases. This measure requires no legislative amendment.

Strengthen Preventive and Technological Measures through Binding Codes of Practice

Drawing on Singapore's experience under the Online Criminal Harms Act 2023, Malaysia should introduce a statutory power enabling the Minister (or the Controller under the Consumer Protection Act 1999) to issue binding codes of practice for online marketplace operators and designated e-commerce platforms. These codes should impose the following minimum obligations: (a) the implementation of reasonable systems (combining automated tools and human review) for the proactive detection and disruption of scam listings, non-delivery risk indicators, and fake reviews; (b) mandatory seller verification (Know-Your-Customer) procedures before listings are permitted; (c) a duty to respond to regulatory directions from KPDN, MCMC or the National Scam Response Centre within a prescribed short timeframe (recommended: 24 to 48 hours); (d) transparency requirements regarding ranking algorithms and paid advertising parameters that may affect consumer choice;

and (e) periodic reporting to the Controller on anti-fraud measures taken, complaint volumes, and resolution outcomes.

Non-compliance with an applicable code of practice should be treated as a breach of the Consumer Protection Act 1999 or the 2024 Regulations, attracting administrative penalties and, where appropriate, secondary liability for consumer losses. In addition, Malaysia should establish a public E-Commerce Platform Safety Rating system, modelled on Singapore's E-commerce Marketplace Transaction Safety Ratings. Platforms would be scored against objective criteria (seller verification standards, speed of scam removal, complaint resolution rates, and cooperation with authorities). The ratings should be published on a government-maintained website to create reputational incentives for higher standards. These measures would shift the Malaysian framework from a predominantly reactive model toward a preventive, technology-enabled system of platform accountability while remaining adaptable to evolving fraud techniques.

Improve Access to Redress and Dispute Resolution

Effective consumer protection requires not only strong substantive rules but also accessible and enforceable remedies. The following targeted reforms are recommended:

(a) Expand the jurisdiction and specialised capacity of the Tribunal for Consumer Claims. The monetary jurisdiction of the Tribunal should be increased for e-commerce claims (recommended: up to RM100,000). Special simplified procedures should be introduced for the most common categories of e-commerce disputes: non-delivery, material discrepancy between advertised and delivered goods, and misleading product descriptions with reduced evidentiary formalities and expedited hearing timelines.

(b) Establish a government-supported Online Dispute Resolution (ODR) platform for e-commerce transactions. A dedicated ODR system should be developed under the supervision of KPDN or the Tribunal. Major online marketplaces should be required to integrate with or recognise the platform. The ODR process should offer staged resolution (negotiation, mediation, and, where necessary, adjudication) and be capable of producing decisions that are enforceable in the same manner as Tribunal awards.

(c) Strengthen the enforcement of Tribunal awards and ODR decisions against platforms and sellers. Where a platform or seller fails to comply with a final award or decision within a prescribed period, the Controller should be empowered to: (i) impose administrative penalties; (ii) order the temporary suspension of the seller's or platform's ability to list goods; and (iii) in the case of platforms, treat persistent non-compliance as a breach of the statutory duty of care, attracting secondary liability for consumer losses.

These measures would significantly improve the practical utility of existing redress mechanisms, reduce the current gap between obtaining an award and actual recovery, and create stronger incentives for platforms to resolve disputes efficiently at an early stage.

Address Cross-Border Challenges

Malaysia should explore mutual assistance arrangements and information-sharing protocols with key trading partners, while simultaneously imposing clearer obligations on platforms that facilitate cross-border sales into the Malaysian market. Platforms should be required to ensure that foreign sellers provide accurate local contact and service-of-process information, and to assist in the execution of consumer remedies where reasonably practicable.

CONCLUSION

The rapid expansion of e-commerce in Malaysia has delivered significant economic benefits, yet it has also exposed serious weaknesses in the country's legal and institutional framework for protecting consumers against fraudulent transactions. Despite the Consumer Protection Act 1999 and the Consumer Protection (Electronic Trade Transaction) Regulations 2024, high complaint volumes, substantial financial losses, and evolving fraud tactics show that the current regime remains insufficient. Comparative analysis with the United Kingdom and Singapore points to clear pathways for improvement. The UK's Digital Markets, Competition and Consumers

Act 2024 demonstrates the value of strong direct administrative enforcement powers, while Singapore's experience shows the benefits of combining statutory rules with practical platform accountability, proactive anti-scam measures, and effective inter-agency coordination. Both jurisdictions have moved toward a more preventive, platform-centred model. Malaysia's framework, although improved in disclosure requirements, still suffers from limited platform liability, weak administrative enforcement tools, fragmented institutional coordination, and weak cross-border effectiveness. The recommendations advanced in this article that is to strengthen platform duties, enhancing administrative powers, improving inter-agency coordination, introducing binding preventive codes, strengthening redress mechanisms, and addressing cross-border challenges, offer a coherent reform agenda. Implementing these measures would enable Malaysia to close existing gaps, strengthen consumer trust and support the sustainable development of its digital marketplace.

REFERENCES

1. Abdul Manap, Norhoneydayatie, Madihah Adnan, Amirah, Zakaria, Zamzuri "Consumer Protection Against Online Purchase Fraud in Malaysia: An Analysis of the Consumer Protection Act 1999" *International Journal of Advanced Research* 10.11(2022)
2. Amin, N., & Mohd Nor, R. (2013). Online shopping in Malaysia: Legal protection for e-consumers. *European Journal of Business and Management*, 5(24), 79.
3. Armizan, M. A. (2026, February 4). Parliamentary reply on online fraud complaints [Oral answer]. Dewan Rakyat, Parliament of Malaysia. Reported in *New Straits Times*: <https://www.nst.com.my/news/nation/2026/02/1371621/armizan-over-33000-online-fraud-complaints-lodged-2023-2025>
4. Cheong, W. L., & Ahmad, M. F. (2023). Understanding the social commerce scam and consumers' self-protection behaviour. *International Journal of Business and Technology Management*, 5(2), 251–262. mohe.gov.my
5. Competition and Markets Authority (CMA) v AA Driving School and BSM Driving School (2026).
6. Competition and Markets Authority. (2026, April 15). CMA orders the AA and BSM driving schools to refund learner drivers over drip pricing. GOV.UK. <https://www.gov.uk/government/news/cma-orders-the-aa-and-bsm-driving-schools-to-refund-learner-drivers-over-drip-pricing>
7. Inter-Ministry Committee on Scams. (2024, April 10). E-commerce Marketplace Transaction Safety Ratings 2024. Ministry of Home Affairs. <https://www.mha.gov.sg/media-room/newsroom/e-commerce-marketplace-transaction-safety-ratings-2024/>
8. Ministry of Home Affairs. (2025, September 26). Enhanced e-commerce guidelines to safeguard consumer trust and foster competitive e-commerce market. <https://www.mha.gov.sg/media-room/newsroom/enhanced-e-commerce-guidelines-to-safeguard-consumer-trust-and-foster-competitive-e-commerce-market>
9. Mohd Khalid, I. (2026, June 15). Statement on online scam cases and losses in 2025. Royal Malaysia Police / reported via *New Straits Times*: <https://www.nst.com.my/news/nation/2026/06/1464407/igp-66204-online-scam-cases-reported-2025>
10. Mohd Mokhtar, M. F. (2025). Consumer ADR in Malaysia. In E. Sahin-Sengul & S. Kaya (Eds.), *Consumer Alternative Dispute Resolution in Emerging Economies* (pp. 188–204). Routledge. <https://doi.org/10.4324/9781032689739-13>
11. Mordor Intelligence. (2026, August). Malaysia e-commerce market growth, share & size - 2031. <https://www.mordorintelligence.com/industry-reports/malaysia-ecommerce-market>
12. Razali, N. A. H., Wan Rosli, W. R., & Othman, M. B. (2022). The legal protection of e-consumers against e-commerce fraud in Malaysia. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, 7(9), e001778. <https://doi.org/10.47405/mjssh.v7i9.1778>
13. Sarabdeen, J. (2025). Empirical analysis of e-consumer laws and way forward for better protection. *Journal of Posthumanism*, 5(4), 1008–1021. <https://doi.org/10.63332/joph.v5i4.1183>
14. Singapore Police Force. (2025, August 30). Mid-year scam and cybercrime brief 2025. <https://www.police.gov.sg/-/media/SPF/Media-Room/Statistics/Mid-Year-Scams-and-Cybercrime-Brief-2025/Police-News-Release---Mid-Year-Scam-and-Cybercrime-Brief-2025.pdf>
15. Subagyono, B. S. A., Satory, A., Suheryadi, B., Melissa, M., Yeri, H. N., & Indiaty, K. A. L. (2025). In the Context of Consumer Protection Law, E-Commerce and Its Settlement: Lesson From Indonesia,

- Malaysia, and European Union. *Journal of Posthumanism*, 5(1), 379–397. <https://doi.org/10.63332/joph.v5i1.567>
16. The Edge Malaysia. (2026, July 2). Over RM430 mil worth of losses to e-commerce scams in the first three months of 2026 — Armizan. <https://theedgemalaysia.com/node/809191>
 17. The Star. (2026, January 26). Online transactions record highest number of complaints. <https://www.thestar.com.my/news/nation/2026/01/26/online-transactions-record-highest-number-of-complaints>
 18. The Vibes. (2026, August 17). E-Commerce fraud surges 92% as Shopee calls for stronger consumer safeguards. <https://www.thevibes.com/articles/lifestyles/126271/e-commerce-fraud-surges-92-as-shopee-calls-for-stronger-consumer-safeguards>
 19. Tseng, Y.-H. (2023). Consumer protection in ASEAN's e-commerce: Common issues and the path towards harmonization of regulatory frameworks. Chulalongkorn University. <https://doi.org/10.58837/chula.the.2023.1248>
 20. Zeno, J. (2022). Information in consumer contracts: Reforming consumer protection law in Malaysia. *Asian Journal of Comparative Law*, 17(2), 242–267. <https://doi.org/10.1017/asjcl.2022.18>