Conference of Bussines, Social Sciences and Technology
31
Vol. 6 Issue 1, 2026, 31-45

Assessing the Adequacy of Malaysian Law in Preventing Online Scams: A Comparison with the United Kingdom

Nur Aleya Aisyah Mat Khalid[1], Izuan Izzaidi bin Azmi[2], Mohamad Hilman Nabil Fakrul Nizam[3], Danish Hakim Kamarul Anuar[4], Nuha Al-Hani Azharar[5]

[1-5]Faculty of Law, Universiti Teknologi MARA, Malaysia
✉ Corresponding email: uitmlegalresearch@gmail.com

History of Article
Submitted : July 18, 2026
Revised : July 25, 2026
Accepted : August 10, 2026
Published : September 22, 2026
DOI : https://doi.org/10.37253/conescintech.v6i1.12702

Copyright© 2026 by Author(s). This work is licensed under a Creative Commons Attribution-Non Commercial-Share Alike 4.0 International License. All writings published in this journal are personal views of the authors and do not represent the views of this journal and the author's affiliated institutions.

Abstract

The issue of Authorised Push Payment (APP) frauds is becoming increasingly prominent in digital banking as they cause substantial harm to society and finances due to manipulation of consumers to make voluntary payments to fraudsters' accounts. Therefore, this issue has brought to light the problems of protecting consumer rights and ensuring proper regulation of the existing frameworks that determine liability distribution between banks and consumers. The main problem in the current study is associated with the lack of the statutory obligation for banks to reimburse losses from such crimes in Malaysia despite the rising level of criminal activity and consumers' susceptibility in the field of digital payments. Protection of consumers under the current legal framework in Malaysia is mainly ensured by the Financial Services Act 2013 and banking regulations as well as financial dispute resolution services; however, no mandatory obligation on banks to reimburse losses related to authorised payments has been introduced. The research has used a doctrinal comparative legal approach as the methodology to review Malaysia's legislative and regulatory frameworks in relation to those applied in the United Kingdom concerning mandatory reimbursement of APP fraud victims. The research is based on legal sources including both Malaysian and comparative ones. The study concludes that the introduction of a mandatory reimbursement framework in Malaysia, informed by comparative analysis of the United Kingdom model, would strengthen consumer protection and improve the allocation of financial risk in APP fraud cases.

Keywords: Authorised Push Payment (APP) Fraud; Consumer Protection; Mandatory Reimbursement; Banking Liability; Digital Banking; Financial Services Act 2013; Comparative Legal Analysis; Electronic Payment Fraud.

Introduction

Digital banking has revolutionized the way in which retail payments can be conducted with regard to their speed,convenience, and accessibility. The same technology has provided an environment that is very scalable for fraud. What is unique about this form of fraud compared to an ordinary unauthorized payment is that it refers to an authorized push payment scam in which a scammer tricks the payer into instructing the bank or the service provider to send funds to an account of the scammer. Although the payment is authorized from a technical perspective, it is done so through manipulation, impersonation, fraudulent investment opportunities, invented emergencies, etc. It is legally important since the ordinary payment rules usually make the bank responsible for any unauthorized transactions while regarding an authorized one as the customers' act (Braithwaite, 2024; Shum, 2025).

Malaysia has come up with a multi-agency approach to address the problem of online financial scams. The National Scam Response Centre works as a coordination mechanism between the National Anti-Financial Crime Centre, Royal Malaysia Police, Bank Negara Malaysia, Malaysian Communications and Multimedia Commission, financial and telecommunication institutions. This agency's jurisdiction covers the instances when money is withdrawn without the knowledge of the account owner and where victims are conned to withdraw money using online financial services (National Anti-Financial Crime Centre [NFCC], n.d.). While this system improves detection and recovery mechanisms, it doesn't provide the right to compensation as such.

The frequency and magnitude of the online fraud reveal a structural flaw in the legal system that relies mainly on prevention, criminal law enforcement, and unauthorised transactions. The Policy Document on Ensuring Fair Treatment for Victims of Unauthorised e-Banking Transactions issued by Bank Negara Malaysia is an example of a joint liability model in case of losses caused by unauthorised transactions (Bank Negara Malaysia [BNM], 2024a). Nevertheless, according to the Annual Report 2025 of BNM, the current compensation model is centred around unauthorised e-banking transactions only (BNM, 2026). Therefore, the APP scam victims find themselves in an ambiguous situation since the payment order was made by the customer himself although manipulated by a fraudster.

The Financial Services Act 2013 (FSA) is the main legislative regime regulating financial institutions, payment systems and financial consumer protection in Malaysia. It is provided under Part VIII of the FSA that BNM has the power to establish standards of business conduct and financial service providers shall not engage in the prohibited business conduct. In particular, section 123 provides that BNM may establish standards that would guarantee that financial service providers will treat consumers fairly, responsibly and professionally whereas section 124 forbids the prohibited business conducts that are set out in Schedule 7 to the Financial Services Act 2013 (ss. 123-124). The above legislative provisions will be relevant for the regulatory directions regarding fairness, disclosure, complaints and responsible behavior. However, there is no provision in the FSA which states that a bank will have to compensate a customer for being deceived into making a money transfer.

The consumer can obtain relief by making a complaint to the bank's internal dispute resolution procedure and, if eligible, via the FMOS which is an independent and impartial dispute resolution service offered free of charge to consumers and investors in the financial markets (Financial Markets Ombudsman Service [FMOS], n.d.). The ombudsman review is very important as it evaluates the conduct, the documents and the fairness without conducting a legal suit. However, it is not the same thing as imposing a statutory presumption for reimbursement. The victim should prove the cause for obtaining relief. The decision will depend on the circumstances and jurisdictional limits involved.

The approach taken by the United Kingdom has been quite distinct. Since 7 October 2024, the requirement to provide APP scam refunds by the Payment Systems Regulator ensures minimum protection to consumers making payments through Faster Payments and CHAPS systems. The key requirement is that the sending payment services provider will refund the victim under certain conditions, within a specified maximum amount, and taking into account a limited definition of the consumer standard of care. The costs involved in the process are equally shared by both parties, the sending and the receiving payment services providers (Payment Systems Regulator [PSR], 2025).

The United Kingdom model changes the legal starting point. Rather than asking a victim to prove that the bank was contractually or tortiously at fault, the regulatory framework begins from reimbursement and permits refusal only in defined circumstances, including fraud by the claimant or gross negligence in failing to satisfy the prescribed standard of caution. Vulnerable consumers receive additional protection. Claims are ordinarily to be resolved within five business days, with a maximum period of thirty-five business days where the payment service provider requires further information (PSR, 2025). The model thus combines victim redress with institutional incentives for fraud detection, intervention and account monitoring.

Scholarly research related to APP fraud has focused on the relationship between consumer discretion and institutional accountability. On one hand, it is argued that consumers should exercise due diligence as the direction is authorized. On the other hand, it is noted that it is easier for banks and payment providers to detect any suspicious payment trends, intervene, and distribute fraud losses across the payment systems. Hence, the issue is about the proper distribution of losses while maintaining incentives for consumers and financial institutions to protect themselves from fraud (Braithwaite, 2024; Shum, 2025). It can be seen that the UK approach considers the second point without dismissing the role of consumers.

The literature in Malaysia, together with policy discourse, has been moving more towards issues such as scam prevention, mules, raising public awareness, securing transactions, and enforcing measures from multiple agencies. There is, however, a definite void in terms of doctrine in the area of authorized payment scams and how these are to be treated legally. The rules governing unauthorized e-banking transactions are not necessarily determinative of who should be liable for losses arising out of an APP scam (BNM, 2024a, 2026).

This research, therefore, examines whether there is sufficient consumer protection from APP frauds under Malaysian laws and the need to borrow features of the United

Kingdom model of compensation into Malaysia. This research has three main aims. First, this research will examine the current laws and regulations in place in Malaysia for protecting consumers suffering from online payment scams. Second, it will make a comparison between the above laws and regulations in Malaysia with the mandatory compensation regime of the United Kingdom. Third, it will suggest a Malaysian compensation system.

The study is limited to APP scams involving domestic electronic transfers and the allocation of financial loss between consumers and regulated payment institutions. It does not attempt to examine every form of cybercrime, criminal prosecution or platform liability. The analysis is also doctrinal rather than empirical. It evaluates legal rules, policies and institutional design but does not independently measure bank reimbursement rates or consumer behaviour. These limits do not reduce the significance of the inquiry because the central issue is normative: which participant in the payment ecosystem should bear the loss when a transaction is authorised in form but induced by fraud?

Research Method

The methodology for this research will be a qualitative doctrinal and comparative approach. Doctrinal research is appropriate for this study since the main issue is related to the content and adequacy of the legal duties and not the statistics related to fraud. In this research, the law will identify the applicable laws, interpret their meaning and determine if there is a clear allocation of duties and responsibility between consumers and banks.

Primary sources from Malaysia include the Financial Services Act 2013, policies on treatment of customers and unauthorised transactions in e-banking issued by Bank Negara Malaysia, the organizational structure of the National Scam Response Centre and the complaint handling mechanism of the Financial Markets Ombudsman Service. Also included will be the legal environment under which banks offer payment services, such as contractual authorization, the standards of business conduct and authorised or unauthorised transactions.

The UK sources consist of the Payment System Regulator's consolidation policy in regards to APP scam reimbursement, the Faster Payments and CHAPS reimbursement schemes, as well as the Payment Services Regulations 2017 and Payment Services (Amendment) Regulations 2024. The above documents will assist in determining the scope of mandatory reimbursement, caution required, time limits, limit per claim, position of vulnerable consumers, as well as liability apportionment between the sending and receiving payment service providers.

Secondary sources refer to academic sources, reports, policy justifications, and institutional guidance. Primarily, emphasis is placed on the use of primary sources and official regulatory sources, given the fact that the law has evolved very quickly after October 2024. Secondary sources are employed to justify the policies, such as loss allocation, moral hazard, incentive for prevention, and capabilities of consumers and financial organizations.

The analysis will be conducted in four phases. First, the research will explain what APP fraud entails and differentiate it from unauthorised payment fraud. Second, it will outline the Malaysian legal system and determine whether the current legislation and regulations form an adequate framework for establishing the right to reimbursement. Third, it will evaluate the United Kingdom legal regime as a functional counterpart. Finally, it will consider which components of the UK system can be adapted in the Malaysian system without assuming that the UK regime must be replicated. Comparative approach is functional in nature as both regimes deal with the same practical issue, a legitimate instruction arising out of fraudulent manipulation.

This aspect of trustworthiness is ensured by triangulating the sources. The statutory law is analyzed alongside the regulation policy and institutional policy guidelines. The prevailing regulations in the UK are matched against the consolidated policy of the Payment Systems Regulator along with consumer guidance. The study does not consider the public awareness campaigns and voluntary banking practices as being legally equal to that of reimbursement duty.

Results and Discussions

The Nature of APP Fraud and the Limits of Traditional Payment Law

The APP fraud exploits the discrepancy between authorization and intention. For the bank, the client has been authorized, verified, and approved for making payments. But the point of view of the victim is different since money transfer happens under deception. The fraudster may impersonate a policeman, bank worker, family member, financial advisor, web shop owner, or employer. The victim's personal information does not need to be disclosed because the victim performs the transfer of money himself or herself. The APP frauds can be defined as those cases where the individual transfers money to the fraudster acting as a legitimate beneficiary, according to the definition by Payment Systems Regulator (PSR, 2025a).

This structure creates a legal classification problem. Rules designed for stolen credentials or unauthorised access are usually triggered when the customer denies giving the payment instruction. In APP fraud, the customer cannot honestly deny authorising the payment. The dispute instead concerns why the instruction was given and whether the sending bank, receiving institution or wider payment system should absorb the resulting loss. A legal regime that treats formal authorisation as conclusive therefore risks overlooking the fraudulent manipulation that caused the customer to initiate the transfer (PSR, 2025a).

The prevention capacities of the parties are unevenly distributed. A consumer has direct knowledge of the conversation with the scammer but may lack information regarding account networks, mule-account behaviour, device patterns, rapid fund dispersal and similar complaints involving the receiving account. Banks possess transaction data, fraud-detection systems, customer profiles and the ability to delay, query or block suspicious payments. Receiving institutions can monitor accounts that receive funds from multiple victims and respond to warnings from sending institutions. This

asymmetry supports a shared-responsibility framework rather than an automatic rule that the deceived payer should bear the entire loss (Bank Negara Malaysia [BNM], 2026; PSR, 2025b).

On the other hand, an efficient reimbursement scheme should not overlook the role of consumers as well. A system that allows compensation of any damage without looking at the conduct of the consumer can have a detrimental effect on the incentives to react to the warnings targeted at him, to give the requested information and report the fraud. The key issue for the regulator is thus one of differentiating ordinary human error induced by manipulation from negligence that is too gross to transfer the damages.
This is critical due to the way in which the fraudster creates a sense of urgency, authority, and emotional appeal. A rule of carelessness that is solely based on whether the consumer could have shown more care will not provide protection in many instances and will have the same flaws as the pre-reform rule. The gross negligence standard maintains a legitimate duty of care on the part of the consumer, but recognizes that the fact alone that the consumer was vulnerable does not mean that all of the losses must be placed at their feet.

The Malaysian Legal and Regulatory Framework

The Financial Services Act 2013 (FSA) constitutes the primary legislation for financial institutions and payment systems in Malaysia. Consumer-protection measures under the FSA enable Bank Negara Malaysia (BNM) to lay down standards of good, responsible, and professional behavior and to prohibit any conduct that is deemed to be unfair (Financial Services Act 2013, ss. 123-124). Such powers facilitate rules pertaining to complaint resolution, disclosure, security controls, and fair treatment; thus, the FSA can be considered the starting point for scam regulation.

Nevertheless, the FSA works primarily as an enabling and supervisory law. It does not mandate financial institutions to compensate victims of APP scams when the transactions were initiated by the customers themselves. Therefore, consumer protection mostly relies on policy documents, contractual agreements, and dispute resolution processes.

BNM's Policy Document on Ensuring Fair Treatment of Victims of Unauthorised e-Banking Transactions enhances the safeguards of unauthorised transactions through the implementation of shared accountability and by discarding the notion that usage of authentic credentials necessarily makes customers liable (BNM, 2024a). However, this policy framework fails to encompass APP scams since in such cases, customers have authorised the payment.

BNM's Annual Report 2025 shows that the compensation framework adopted in 2024 only covers unauthorised e-banking transactions despite the fact that the need for enhanced consumer protections and shared liability is acknowledged (BNM, 2026). Likewise, BNM's Policy Document on Fair Treatment of Financial Consumers fosters transparency and good behavior but does not provide any guidelines for reimbursement, fixed compensation deadlines or shared cost liabilities (BNM, 2024b).

Other methods offer some level of protection. The NSRC ensures that there is a prompt response aimed at tracking down and recovering money lost due to fraud (NFCC, n.d.), while the FMOS ensures that there is access to a dispute resolution mechanism (FMOS, n.d.). Recovery is different from reimbursement; the decisions made by the ombudsmen are also reactive and case-specific.

There are possibilities of suing banks through contract and negligence for non-compliance with regulations and their policies, but such legal avenues are expensive and fact-specific. Criminal law ensures that fraudsters and the operators of mule accounts are punished, but criminal law has no bearing on who suffers the economic loss.

As a whole, Malaysia has created prevention measures, regulations and dispute resolution mechanisms, however its model is still remedial. The lack of a well-defined compensation scheme for APP frauds leads to uncertainty on part of customers and fails to motivate institutions to prevent fraud and identify mule accounts.

The United Kingdom Mandatory Reimbursement Model

The United Kingdom established an obligatory compensation scheme for qualified Authorised Push Payment (APP) frauds via Faster Payments and CHAPS as of 7 October 2024. Under this scheme, it is the responsibility of the payment service provider that sends payments to compensate victims, providing an easy way to do so (PSR, 2025b). However, this scheme does not go further than necessary. It does not cover civil matters, payments sent abroad, payments that happen outside of the designated payment system, or payments done for illegal reasons (PSR, 2025b).

There exists a balance between consumer protection and institutional limitations. The maximum amount of compensation in each claim is limited to £85,000, and the provider may impose an excess fee of no more than £100 unless the person was vulnerable and it affected his/her ability to protect himself or herself from fraud (PSR, 2025b). Compensation must be made within five working days, but this time limit may be increased if extra information is needed, not exceeding thirty-five working days (PSR, 2025b).

Caution of the consumer has been made narrowly defined. Reimbursement can be denied only when the consumer had committed fraud or if the consumer was non-vulnerable and had committed gross negligence by not adhering to the requirements stipulated in the law (PSR, 2025b). Gross negligence entails more than negligence. Additionally, service providers are not at liberty to enter into other contracts that go against the statutory provision.

A key structural feature is the 50:50 cost-sharing mechanism between sending and receiving payment service providers (PSR, 2025a, 2025b). This reflects the ability of receiving institutions to detect suspicious account activity and discourages either side from relying solely on the other to prevent fraud. The Payment Services (Amendment) Regulations 2024 further support prevention by allowing providers, in specified circumstances, to delay payment execution where fraud or dishonesty is reasonably suspected.

Early outcomes indicate practical effectiveness. According to the PSR's reimbursement dashboard updated on 11 June 2026, approximately 89% (£243 million) of losses in reimbursable APP scam claims were returned to victims between 7 October 2024 and 31 December 2025. The PSR also reported that 82% of claims were resolved within five business days and 98% within thirty-five business days (PSR, 2026).

Overall, the UK model treats APP scam losses not merely as individual consumer losses but as a payment-system risk. By linking reimbursement with institutional responsibility, the framework strengthens both consumer protection and incentives for fraud prevention.

Comparative Assessment of Malaysia and the United Kingdom

Issue	Malaysia	United Kingdom
Legal starting point	No general mandatory reimbursement right for APP scams; claims depend on recovery, bank assessment, conduct standards or dispute resolution.	Mandatory reimbursement is the starting point for in-scope APP scam claims, subject to defined exceptions and limits.
Transaction coverage	Strongest express policy protection currently focuses on unauthorised e-banking transactions.	Specific protection for authorised payments induced by APP fraud through Faster Payments and CHAPS.
Timeframe	No single universal statutory deadline specifically governing APP reimbursement.	Ordinarily five business days; extended assessment generally capped at thirty-five business days.
Consumer conduct	Responsibility assessed through bank processes, contractual terms and general fairness considerations.	Exhaustive standard of caution; refusal requires fraud or gross negligence, with special protection for vulnerability.
Loss allocation	No universal rule sharing reimbursement liability between sending and receiving institutions.	General 50:50 sharing between sending and receiving payment service providers.
Dispute resolution	Internal complaints and Financial Markets Ombudsman Service may provide case-specific redress.	Mandatory scheme operates first; complaint and ombudsman mechanisms remain available for disputes.

Preventive incentives	Regulatory controls and enforcement exist, but reimbursement costs are not systematically attached to both ends of the payment chain.	Financial liability incentivises both sending and receiving providers to prevent scams and detect mule accounts.

This comparison clearly illustrates that the major flaw in the Malaysian legislation lies not in the lack of any regulation whatsoever. On the contrary, there is no particular provision dealing with the nature of authorized APP fraud. The regulations regarding unauthorized access, criminal liability and post-fraud recovery deal with the other issues but do not define the party which should cover the loss in case the fraud is authorized and confirmed by the victim himself. At the same time, the current system of compensation in Bank Negara Malaysia (BNM) still concentrates on unauthorized e-banking operations (Bank Negara Malaysia [BNM], 2026).

The UK approach is much better in terms of certainty, timeliness, and institutional incentives. Consumers know the right path of redress to make a claim, payment service providers know what timeframes apply, and sending and receiving institutions face economic consequences. Additionally, the approach introduces a systematic process for testing the conduct and vulnerabilities of consumers. Reimbursement happens within five business days and the cost is usually shared equally by the sending and receiving payment service providers (Payment Systems Regulator [PSR], 2025a, 2025b).

However, the United Kingdom model should not be transplanted mechanically. Malaysia's banking market, payment infrastructure, scam typologies, levels of digital literacy, enforcement capacity and institutional arrangements differ. A local framework must be integrated with BNM's supervisory powers under the Financial Services Act 2013, the National Scam Response Centre (NSRC), domestic payment operators and the Financial Markets Ombudsman Service (Financial Services Act 2013; National Anti-Financial Crime Centre [NFCC], n.d.; Financial Markets Ombudsman Service [FMOS], n.d.).

Moral hazard is another issue. Mandatory reimbursement may lead certain consumers to ignore the warning signs or even fraudulent claims. In the United Kingdom, verification of claims, consumer's duty of care, reporting to the police, and consumer participation in the fraud can serve as exceptions to the mandatory reimbursement. There might also be instances when reimbursement will not be granted to a non-vulnerable consumer due to gross negligence regarding consumer's duty of care (PSR, 2025a). Such provisions can also be implemented by Malaysia without adopting a general ordinary negligence defense provision.

The other problem is that of cost. Banks and payments services will shift the burden of reimbursing and complying with requirements onto the consumer via higher charges and restrictions on payment procedures. But the current system also entails very large costs for the victim, the family, enforcement authorities, and society's trust in digital

banking. The pertinent policy question thus is not whether the cost of APP fraud exists, but rather which participant can best prevent, incur, and spread those costs.

Financial institution's capacity to spread loss risks, analyze transaction data, and purchase fraud-detection technologies justifies institutional liability to some degree. For the receiving organizations, in particular, to remain financially neutral in cases when accounts controlled by them repeatedly receive fraud money is not appropriate. The cost-sharing model adopted in the United Kingdom combines victim reimbursement with prevention by making each side of the payment chain responsible for reimbursements (PSR, 2023, 2025b).

The Malaysian framework is consequently inadequate in a specific sense: it does not provide a predictable, mandatory and integrated remedy for APP scam victims. It may be adequate for the general supervision of banks and the treatment of unauthorised transactions, but those functions do not close the reimbursement gap affecting authorised payments induced by fraud (BNM, 2024, 2026).

Proposed Malaysian APP Scam Reimbursement Framework

Malaysia requires that there be a reimbursement policy standard under BNM in relation to APP scams in accordance with BNM’s powers provided under Sections 123 and 124 of Financial Services Act 2013 as well as by legislation. These sections empower BNM to prescribe standards of business conduct and prohibit specific types of unfair conduct concerning financial consumers (Financial Services Act 2013, ss. 123-124). The existence of the policy standard will allow for an immediate start while explicit mention in the legislation will add further certainty and prevent any allegation that the reimbursement is discretionary on the part of BNM.

First, the proposed policy framework needs to define an APP scam as a domestic electronic payment made by a consumer under the misrepresentation of the identity of the recipient or nature of the transaction. Such definition must exempt legitimate civil disputes, transactions made for illegitimate reasons, and first party frauds. This is in line with the UK’s definition of APP scam, distinguishing qualifying APP scams from civil disputes and fraudulent claims made by the victim (PSR, 2025a).

Secondly, the sending financial institution should bear the role of point of contact. It should process claims that meet the requirements within five working days, barring certain exceptions, with a general time limit of thirty-five working days. The proposed timeline is similar to that of the United Kingdom and will ensure that the consumers have an efficient way of making a claim without being passed from the sending and the receiving providers (PSR, 2025a, 2025b).

The third consideration is that the maximum reimbursable amount must be based on evidence and should be evaluated from time to time. Malaysia is not obligated to adopt the standard for maximum reimbursement adopted by the United Kingdom at the rate of £85,000. Nonetheless, the BNM must establish a standard of ringgit in light of the loss statistics in relation to fraud, consumer account transactions, and the ability of the financial industry to handle such losses. There may be a provision of excess claim; nonetheless, there must be no excess claim among vulnerable consumers or low-value

claims where the effectiveness of consumer protection would be jeopardized. In the United Kingdom regime, an excess claim of £100 may be made.

Finally, refusal must be allowed exclusively in instances of first-party fraud or gross negligence. The standard that should be applied needs to be an exhaustive one that requires proof of a total disregard for a particular measure of protection that could have been taken. Being careless, being embarrassed, being older, being unfamiliar with online banking, or being deceived by the scam should not necessarily be reason enough to disallow compensation. In the UK system, gross negligence is a stringent standard and it is supposed to apply only in rare instances (PSR, 2023, 2025a).

Fifth, express protection must be given to vulnerability. Vulnerability can stem from age, disability, lack of fluency in the relevant language, grief, financial stress, cognitive dysfunction, or situational coercion. The question that ought to be considered here is whether the vulnerability had a material impact on the ability of the individual to perceive or fight against the fraud. In this regard, financial institutions need to take into account any such vulnerability in their design of intervention strategies and assessment of refund claims.

The sixth recommendation is for reimbursement costs to be split between the sender and receiver institutions. An allocation of 50:50 would serve as a reasonable starting point and offer preventive incentives to both parties involved in the process. Later, BNM may modify this allocation based on any evidence clearly showing that one party did not adhere to the set standards aimed at fraud prevention. Reimbursements recovered from the fraudster or mule account need to be credited against the reimbursement costs in order to avoid double compensation.

Seventhly, receiving institutions need to be obligated to perform express duties related to preventing mule-account schemes. Such duties may include intensified surveillance of any unusual patterns in the inflow of payments, quick action upon the receipt of proven scam warnings, temporary suspension of the accounts in case certain risk criteria are fulfilled, as well as retention of appropriate transaction information.

The eighth component in this regard is that the reimbursement scheme has to be linked up with the NSRC. This will entail that a notification sent to the sending organization will have to result in almost instant notification to the receiving organization and, where appropriate, to the NSRC. The consumer should not be made to go through multiple reporting lines before a claim will even be considered, but a reasonable effort to cooperate with information requests and reporting to the police may form part of the standard of caution for the consumer.

Nine, the FMOS must be allowed sufficient resources to facilitate its evaluation of any rejected claims, delays, and vulnerabilities assessments. The financial institutions must give written reasoning for any rejection of claims that is justified by the evidence and the exceptions available for such a review. Additionally, all information regarding the number of claims, reimbursement levels, delays in processing, grounds of rejection, and recovered money must be made public. Currently, the FMOS offers an independent and free dispute resolution process for eligible financial consumers and investors (FMOS, n.d.).

Lastly, any reform in relation to reimbursement needs to be an adjunct, not a substitute, for prevention. Payee confirmation, cooling-off period for transactions, risk-based payment delays, prominent and customized warnings, account name matching, behavioral analysis, as well as closer cooperation with telecommunications and platform providers are all still needed. Payment Services (Amendment) Regulations 2024 have introduced changes to the legislation governing UK payment services, allowing payment service providers to delay certain outbound payments if there are reasonable grounds to doubt that fraud or dishonesty have occurred.

A phased implementation would be appropriate. BNM could initially apply the framework to domestic retail transfers involving individuals and microenterprises, collect compliance data for a period of twelve to eighteen months and subsequently review the reimbursement limit, cost-sharing mechanism and regulatory scope. Independent evaluation should consider reimbursement outcomes, fraud displacement, false claims, the treatment of vulnerable consumers and whether financial institutions are improving their preventive controls.

Conclusion

The study has discovered that Malaysia has set up relevant institutions and regulation systems to counteract the menace of internet scams: however, the legal coverage for the victims of the APP scam is still lacking. Under the Financial Services Act 2013, Bank Negara Malaysia has the authority to regulate business practices, and the fair treatment approach facilitates consumer protection. Besides, there is a regulation for unauthorized e-banking transactions that facilitates mutual responsibility and the NSRC facilitates swift action while the Financial Markets Ombudsman Service facilitates dispute resolution. However, these do not provide the right to reimbursement in case of deception.

The research results suggest that although there is institutional infrastructure and regulation in place in Malaysia to protect against online fraud, existing laws that protect victims from Authorised Push Payment frauds are inadequate. In spite of the ability of Bank Negara Malaysia to regulate the standards of business conduct and consumer protection under the Financial Services Act 2013, as well as specific regulations on unauthorised transactions in electronic banking by means of shared responsibility, this does not cover authorised payments made as a result of deception. Moreover, in spite of the existence of the NSRC and a means of dispute resolution offered by the Financial Markets Ombudsman Service, there is no statutory provision for a refund of the victims of manipulation.

The distinction between unauthorised transactions and authorised payments induced by fraud is the central weakness. A framework designed around stolen credentials cannot adequately resolve loss allocation when the victim personally authenticates the transfer. Reliance on recovery, voluntary bank decisions or case-specific complaints produces uncertainty and inconsistent protection.

The United Kingdom model demonstrates a more coherent alternative. It begins with mandatory reimbursement for in-scope claims, imposes short decision deadlines,

protects vulnerable consumers, limits refusal to fraud or gross negligence and shares reimbursement costs between sending and receiving payment service providers. Its early operation indicates that high reimbursement rates and timely resolution are achievable.

Malaysia should therefore adopt a dedicated APP scam reimbursement framework under Bank Negara Malaysia's regulatory authority, supported by statutory amendment where needed. The framework should define APP fraud, establish the sending institution as the claim point, prescribe deadlines, protect vulnerability, use a gross-negligence threshold and allocate costs between sending and receiving institutions. It should also integrate with the NSRC and permit independent review by the Financial Markets Ombudsman Service.

The proposed reform would not make banks insurers against every poor decision. Proper exclusions, claim verification and an exhaustive standard of caution can address moral hazard and first-party fraud. The purpose is to allocate loss according to preventive capacity and to ensure that institutions controlling the payment infrastructure have a direct incentive to detect scams and mule accounts.

Any future research efforts should empirically validate the suggested model using data from Malaysian insurance claims, as well as the costs and experiences of both victims and institution compliance. Special attention must be paid to vulnerable consumers, microenterprises, e-wallet payments, and the involvement of telecommunication and digital platforms. A more generalized shared responsibility approach might be necessary in the future, but mandatory reimbursement is the first step.

References

Bank Negara Malaysia. (2013). Financial Services Act 2013 (Act 758). https://www.bnm.gov.my/documents/20124/820862/Financial%2BServices%2BAct%2B2013.pdf

Bank Negara Malaysia. (2024). Ensuring fair treatment for victims of unauthorised e-banking transactions. https://www.bnm.gov.my/-/pd-fair-treatment24

Bank Negara Malaysia. (2024). Fair treatment of financial consumers. https://www.bnm.gov.my/documents/20124/938039/pd-ftfc-mar24.pdf

Bank Negara Malaysia. (2025). Building a united front against online fraud risk. https://bnm.gov.my/ar24b7

Bank Negara Malaysia. (2026). Fraud resolution: Building trust through shared accountability. https://bnm.gov.my/publications/ar2025/box4

Financial Conduct Authority. (2024). FG24/6: Guidance for firms that enables a risk-based approach to payments. https://www.fca.org.uk/publications/finalised-guidance/fg24-6-guidance-firms-enables-risk-based-approach-payments

Financial Markets Ombudsman Service. (n.d.). Financial Markets Ombudsman Service. https://www.fmos.org.my/

HM Treasury. (2024). The Payment Services (Amendment) Regulations 2024: Policy note. https://www.gov.uk/government/publications/the-payment-services-amendment-regulations-2024-policy-note

National Anti-Financial Crime Centre. (n.d.). National Scam Response Centre. https://nfcc.jpm.gov.my/index.php/en/about-nsrc

Payment Systems Regulator. (2023). Fighting authorised push payment fraud: A new reimbursement requirement (PS23/3). https://www.psr.org.uk/media/iolpbw0u/ps23-3-app-fraud-reimbursement-policy-statement-final-june-2023.pdf

Payment Systems Regulator. (2023). Fighting authorised push payment scams: Final decision (PS23/4). https://www.psr.org.uk/media/kwlgyzti/ps23-4-app-scams-policy-statement-dec-2023.pdf

Payment Systems Regulator. (2024). Faster Payments APP scams reimbursement requirement: Confirming the maximum level of reimbursement (PS24/7). https://www.psr.org.uk/publications/policy-statements/ps247-faster-payments-app-scams-reimbursement-requirement-confirming-the-maximum-level-of-reimbursement/

Payment Systems Regulator. (2025). APP scams reimbursement requirement: Consolidated policy statement (PS25/5). https://www.psr.org.uk/media/rhelv4op/ps25-5-app-scams-reimbursement-consolidated-policy-statement-may-2025.pdf

Payment Systems Regulator. (2026). APP scams reimbursement dashboard for Q4 2025. https://www.psr.org.uk/information-for-consumers/app-scams-reimbursement-dashboard/

United Kingdom. (2017). The Payment Services Regulations 2017, SI 2017/752. https://www.legislation.gov.uk/uksi/2017/752/contents

United Kingdom. (2024). The Payment Services (Amendment) Regulations 2024. https://www.legislation.gov.uk/ukia/2024/145/pdfs/ukia_20240145_en.pdf

Acknowledgments

The authors would like to express their appreciation to the Faculty of Law, Universiti Teknologi MARA, for providing the academic environment and research facilities that supported the preparation of this article. The authors also acknowledge the guidance and comments received from their academic instructors and peers. No external funding was received for this research.

Competing Interest

The authors state that there is no conflict of interest in the publication of this article.

Generative AI Statement

During the preparation of this manuscript, the authors used ChatGPT by OpenAI to assist in structuring the manuscript, refining language and improving readability. Following this process, the authors critically reviewed, edited and validated the output against primary legal and regulatory sources to ensure accuracy and academic integrity. The authors maintain full accountability for the final content. Generative AI was used

solely as a supportive tool and is not credited with authorship. No legal conclusion was adopted without human review and oversight.

E-ISSN: 2808-5485
Available online at website: https://journal.uib.ac.id/index.php/conescintech/index