Research Journal in Advanced Humanities

RJAH

https://doi.org/10.58256/w868mk83

Open Access

Check for updates

RESEARCH ARTICLE **Section:** *Digital Humanities*

Civil compensation and loss allocation in authorised push payment fraud: Moving beyond criminalisation in instant payment systems—a comparative study of Jordan and the UK

Reem Soud Samawi[1], Rami Omar Abu Rukba[2], Ruba Mohammad Hmaidan[3], Amani Aldabbas[4], Ahmad Albadawi[5] & Baker M. R. Sweilmieen[6]

[1]Al-Balqa Applied University, Jordan

[2]Faculty of Law, Al-Ahliyya Amman University, Jordan

[3]Faculty of Law, Applied Science Private University, Jordan

[4]Lecturer in Law, Lawyer and Legal Consultant

[5]Faculty of Law, Arab Amman University, Jordan

[6]Private Legal Practice (Law Office), Jordan

*Correspondence: reemsamawi3@gmail.com

ABSTRACT

The rapid expansion of instant payment systems has transformed retail finance by enabling real-time, irrevocable transfers, while exposing users and institutions to heightened financial crime risks. A key threat is authorised push payment (APP) fraud, where victims are deceived into authorising transfers to fraudsters. This article argues that financial crime in instant payment systems represents a structural risk that cannot be addressed through criminalisation and anti-money laundering compliance alone. Using a comparative legal and regulatory methodology, it examines Jordan's CliQ system and the United Kingdom's Faster Payments framework to assess responses to APP fraud and related money laundering risks.

The analysis shows that Jordan's framework prioritises system integrity, prevention, and criminal enforcement, but lacks mechanisms for compensating victims of authorised payment fraud, effectively externalising losses onto individuals. By contrast, the United Kingdom has shifted toward systemic accountability through a mandatory reimbursement regime, redistributing losses across payment service providers rather than leaving them with consumers. This shift reflects recognition of regulatory failure in traditional loss allocation within real-time payment systems.

Situating APP fraud within debates on loss allocation, victim protection, and institutional responsibility, the article contributes to scholarship on financial crime governance in digital payments. It proposes a calibrated reform pathway for Jordan, advocating a limited, conditional reimbursement framework that enhances consumer protection without undermining payment finality, criminal enforcement, or anti-money laundering objectives, offering policy-relevant insights for jurisdictions implementing instant payments.

KEYWORDS: Instant payment systems, authorised push payment fraud, financial crime, money laundering, loss allocation, victim compensation, CliQ, Faster Payments, Jordan, United Kingdom

Research Journal in Advanced Humanities

Volume 7, Issue 1, 2026

ISSN: 2708-5945 (Print)

ISSN: 2708-5953 (Online)

ARTICLE HISTORY

Submitted: 01 **January 2026**

Accepted: 09 **February 2026**

Published: 17 **March 2026**

HOW TO CITE

Samawi, R., Abu Rukba, R., Hmaidan, R., Aldabbas, A., Albadawi, A., & Sweilmieen, B. (2026). Civil compensation and loss allocation in authorised push payment fraud: Moving beyond criminalisation in instant payment systems—a comparative study of Jordan and the UK. *Research Journal in Advanced Humanities*, 7(1). https://doi.org/10.58256/w868mk83

Published in Nairobi, Kenya by Royallite Global, an imprint of Royallite Publishers Limited

Introduction

Digital payment systems offering instant fund transfers have expanded rapidly across jurisdictions, delivering significant efficiency gains while simultaneously generating new and complex criminal risks (Hartmann et al., 2019; Górka, 2025). These 24/7 real-time payment platforms—most notably the United Kingdom's Faster Payments Service (FPS) and Jordan's CliQ system—enable bank customers to send and receive funds within seconds, fundamentally reshaping retail payment behaviour (European Central Bank, 2019). However, the acceleration and irrevocability of instant payments have also created fertile ground for fraud schemes that exploit these very characteristics (Ngan, 2025; McKinsey, 2022).

A clear global shift has emerged from traditional unauthorised payment fraud—such as stolen cards or account takeovers—towards authorised push payment (APP) fraud, in which victims are manipulated through social engineering into willingly authorising transfers to criminals (Braithwaite, 2024; Barillà, 2024). These scams, frequently involving impersonation of banks, government authorities, or trusted commercial entities, present acute challenges for legal systems built around the dichotomy between authorised and unauthorised transactions. Once an instant payment is executed, funds can be rapidly dissipated through mule accounts or layered across multiple transfers, leaving victims with limited practical remedies under legal frameworks that were not designed for real-time settlement environments (European Central Bank, 2019; Bello et al., 2025).

Regulators and law enforcement agencies have therefore increasingly recognised that instant payment fraud constitutes a structural risk rather than merely a collection of isolated criminal incidents. The United Kingdom's experience is particularly instructive in this respect. The UK has consistently reported among the highest levels of digital payment fraud in Europe, a trend closely associated with the early adoption of Faster Payments and high levels of digital banking penetration (UK Finance, 2024; Ngan, 2025). By 2024, total annual losses from payment fraud were estimated at approximately £1–1.2 billion, encompassing more than 3.3 million incidents, prompting official recognition of fraud as one of the most serious threats to the UK financial system (National Audit Office, 2023). APP fraud, in particular, has overtaken card fraud in both frequency and value, becoming the dominant category of payment fraud in the UK (UK Finance, 2024).

For an extended period, however, UK regulators and banks approached APP fraud primarily through a responsibilisation framework, emphasising consumer vigilance and education while providing reimbursement only on a discretionary or voluntary basis (Braithwaite, 2024). This position was reinforced doctrinally by the UK Supreme Court's decision in *Philipp v Barclays Bank UK plc* [2023] UKSC 25, which confirmed that banks generally owe no duty to prevent customers from executing authorised payment instructions, even where those instructions result from deception. It was only in response to mounting consumer harm and sustained policy pressure that UK authorities adopted a markedly different approach: reallocating losses away from victims through a mandatory reimbursement regime for APP scam victims, embedded within the Faster Payments scheme rules and overseen by the Payment Systems Regulator (Pay.UK, 2024; Payment Systems Regulator, 2023). This regulatory turn reframes APP fraud not merely as a matter for criminal prosecution, but as a failure of payment system design that warrants collective responsibility and regulatory correction.

By contrast, Jordan's approach to instant payment fraud reflects a more traditional legal posture. Jordan's instant payment system, CliQ, was launched under the supervision of the Central Bank of Jordan (CBJ) and is operated by the Jordan Payments and Clearing Company (JoPACC) as part of a broader national strategy to modernise retail payments and enhance financial inclusion (Central Bank of Jordan, 2022; JoPACC, 2023). The system has rapidly expanded in both user base and transaction volume, and Jordanian authorities consistently emphasise its technical security and traceability, attributing most fraud incidents to user deception rather than systemic vulnerabilities (Central Bank of Jordan, 2024). Official figures indicate that reported fraud losses associated with CliQ remained below JD 100,000 up to mid-2024, out of total transactions exceeding JD 8.3 billion (Central Bank of Jordan, 2024).

Nevertheless, comparative experience suggests caution in interpreting low reported fraud figures at early stages of adoption. Empirical studies indicate that fraud often lags behind widespread uptake of instant payment systems, as criminal networks adapt gradually to new infrastructures (McKinsey, 2022; Górka, 2025). In response to emerging incidents, the CBJ and the Association of Banks in Jordan have prioritised public awareness campaigns, repeatedly warning customers against sharing one-time passwords or account credentials with unknown callers (Association of Banks in Jordan, 2024). At the same time, Jordan has strengthened its

punitive framework by criminalising cyber-fraud and increasing penalties under the Cybercrime Law of 2023, signalling a firm commitment to deterrence and prosecution (Jordan Cybercrime Law No. 17 of 2023).

This framework, however, reveals a critical asymmetry. While Jordan's legal regime robustly addresses system security, AML compliance, and criminal punishment, it provides no equivalent mechanism for victim redress in cases of authorised payment fraud. (Al-Kasassbeh et al., 2024) Where a customer is deceived into initiating a CliQ transfer, the law offers sanctions against the offender but no guarantee of financial recovery for the victim. Banks and payment service providers are not subject to any legal obligation to reimburse authorised fraud losses, and recovery depends largely on the identification of the perpetrator or the voluntary cooperation of the recipient institution (Al-Batoush, 2024; Jordanian Law Portal, 2023). As a result, the financial consequences of APP fraud are effectively externalised onto individual users.

The juxtaposition of the UK and Jordanian experiences therefore raises a central question of public policy and law: how should legal systems regulate financial crime risks inherent in instant payment systems, and what lessons can Jordan's CliQ framework draw from the UK's regulatory shift toward mandatory reimbursement for authorised push payment fraud? This article addresses that question through a comparative legal analysis. Part I maps the relevant literature and identifies a persistent gap between technological fraud mitigation research and legal discussions of liability and compensation. Part II examines Jordan's instant payment framework as a model of criminalisation without compensation. Part III analyses the UK's encounter with APP fraud and the regulatory evolution culminating in mandatory reimbursement. Part IV undertakes a structured comparison of the two regimes, focusing on risk allocation, victim protection, and enforcement incentives. Part V develops policy implications and proposes calibrated reform options for Jordan that seek to balance fraud deterrence, consumer protection, and the integrity of instant payment settlement. Throughout, the article remains anchored in the criminal dimension of financial fraud and money laundering in digital payment systems, while demonstrating that punishment and compliance alone are insufficient to address harms generated by real-time payment infrastructures.

Mapping the Literature and the Research Gap

A substantial body of scholarship examines fraud and money laundering in digital payment systems from technological and empirical perspectives. Within this strand, researchers in computer science, fintech, and financial analytics have concentrated on the development of fraud detection and prevention tools, particularly through artificial intelligence and machine learning models designed to identify anomalous transaction patterns in real time (Bello et al., 2025; McKinsey, 2022). These studies emphasize the growing necessity of advanced data analytics as cashless transactions proliferate at scale. The United Kingdom's rapid transition towards contactless and mobile payments—exceeding 48 billion cashless transactions in 2023—has been accompanied by a corresponding surge in fraud incidents, reinforcing industry expectations that AI-driven monitoring and behavioural analytics will play a central role in mitigating risk (UK Finance, 2024; Ngan, 2025). Industry and consultancy reports similarly underscore that payment service providers must invest heavily in transaction monitoring, customer authentication, and anomaly detection infrastructures to respond effectively to increasingly sophisticated fraud typologies (McKinsey, 2022; ECB, 2019).

Parallel empirical research has explored the relationship between digital payments and money laundering risk. Cross-country analyses suggest that the expansion of digital payment instruments, when coupled with strong rule-of-law institutions, may reduce money laundering by enhancing transaction traceability and limiting the anonymity associated with cash-based economies (Górka, 2025; Hartmann et al., 2019). Digital payment systems generate audit trails that can, in theory, facilitate financial intelligence and enforcement efforts. At the same time, this literature consistently acknowledges the adaptive capacity of criminal networks, which exploit digital infrastructures through techniques such as transaction structuring, the use of mule accounts, and the integration of cryptocurrencies or cross-platform transfers to obscure illicit proceeds (Bello et al., 2025; Ngan, 2025). Notably, however, this technological and empirical literature tends to conceptualise fraud primarily as a problem of system efficiency, detection accuracy, and compliance performance. It rarely extends its analysis to the legal consequences that follow successful fraud events, particularly the allocation of losses and the availability of remedies for victims once preventive mechanisms fail.

Legal scholarship on financial crime in digital payment systems has developed along a partially parallel

but distinct trajectory. Much of the legal literature focuses on criminalisation, enforcement, and regulatory compliance, examining whether existing criminal laws adequately capture new forms of cyber-fraud and whether anti-money laundering frameworks remain effective in increasingly digitised financial environments. In the Jordanian context, for example, legal analyses have highlighted how the Cybercrime Law of 2023 introduced specific offences for online fraud and imposed stricter penalties in response to the expansion of electronic transactions, reflecting a broader trend towards modernising penal frameworks to address cyber-enabled financial crime. Similarly, extensive doctrinal and regulatory commentary addresses AML and counter-terrorist financing obligations, particularly the duties imposed on banks and payment service providers to conduct customer due diligence, monitor transactions, and report suspicious activity (ECB, 2019; Górka, 2025). These measures are widely regarded as indispensable for preventing instant payment systems from being misused for laundering illicit funds or financing terrorism.

Yet the legal literature also reveals important limitations. Traditional criminal law and AML regimes are inherently reactive and incident-focused: they address wrongdoing after it has occurred through investigation, prosecution, and sanctions, but they do not necessarily provide effective remedies for victims of fraud. A defrauded customer may initiate a criminal complaint, but the legal system's primary concern remains the punishment of the offender rather than the restitution of the victim's losses. AML tools may enable authorities to trace or freeze funds in certain cases, but the speed and finality of instant payments often render recovery uncertain once funds have been transferred. Moreover, scholarship examining private law remedies has identified significant doctrinal gaps in the context of authorised payment fraud. In the United Kingdom, attempts to ground bank liability in the common law duty articulated in *Quincecare* have ultimately failed in the context of APP fraud. The Supreme Court's decision in *Philipp v Barclays Bank UK plc* [2023] UKSC 25 confirmed that where a payment is authorised by the customer—even if induced by deception—the bank's core obligation is to execute the instruction, and no general duty exists to protect customers from the consequences of their authorised decisions (Braithwaite, 2024; Barillà, 2024). Commentators have criticised this outcome for leaving victims unprotected and for placing an unrealistic burden on individuals to detect increasingly sophisticated scams (Ngan, 2025).
Regulatory initiatives have sought to fill this gap, but early efforts have been uneven. The United Kingdom's Contingent Reimbursement Model (CRM) Code, introduced in 2019, represented a significant step toward compensating victims of APP fraud, yet its voluntary nature and partial adoption resulted in inconsistent protection and unequal outcomes across institutions (Braithwaite, 2024). Scholarly and policy assessments of the CRM Code converged on the conclusion that voluntary frameworks were insufficient to address a phenomenon that had become systemic in scale and impact. As a result, legal analysis has increasingly acknowledged that instant payment fraud cannot be adequately addressed through individual vigilance, ex post criminal enforcement, or fragmented regulatory initiatives alone.

Despite this growing recognition, a significant gap remains in the academic literature. There is a lack of sustained comparative legal analysis that explicitly links the design of instant payment systems to the allocation of fraud losses and the protection of victims. While technical studies offer valuable insights into fraud prevention and detection, and legal analyses clarify the boundaries of criminal liability and regulatory compliance, relatively few works examine how payment system architecture itself shapes legal responsibility for loss. In particular, the question of who should bear the financial consequences of APP fraud—the victim, the sending institution, the receiving institution, or the financial system collectively—raises normative and policy issues that extend beyond conventional fraud law. The United Kingdom's move towards mandatory reimbursement for APP scam victims constitutes a novel regulatory intervention whose broader implications remain underexplored in the literature, especially when contrasted with jurisdictions such as Jordan, where no equivalent loss-allocation mechanism exists.

This article seeks to address that gap through a comparative, policy-oriented legal analysis of Jordan's CliQ system and the UK's Faster Payments framework. By examining how different regulatory models allocate responsibility for authorised payment fraud and intersect with AML enforcement, the analysis moves beyond descriptive accounts of fraud techniques or isolated doctrinal debates. Instead, it evaluates how legal design choices affect the overall governance of financial crime risks in instant payment systems. In doing so, the article contributes to an emerging global conversation on how legal systems can ensure that instant payments—now increasingly the default mode of retail finance—remain not only efficient and secure, but also resilient to abuse

and fair in their treatment of victims, particularly in emerging and developing economies undergoing rapid digital transformation.

Jordan's Instant Payment Framework: Criminalisation without Compensation

Over the past decade, Jordan has pursued an ambitious programme of payment system modernisation under the leadership of the Central Bank of Jordan (CBJ), with the dual objectives of enhancing financial inclusion and promoting digital finance (Central Bank of Jordan, 2022; Central Bank of Jordan, 2024). A pivotal legal foundation for this transformation was established through the Electronic Payment and Money Transfer Bylaw No. 111 of 2017, which authorises the operation of electronic payment systems by both banks and non-bank entities under CBJ supervision. In conjunction with Article 50 of the Central Bank Law, as amended in 2016, this framework enabled the creation of the Jordan Payments and Clearing Company (JoPACC) as a specialised operator responsible for implementing and managing national payment infrastructures.

Within this institutional architecture, JoPACC operates CliQ, Jordan's instant payment system, which facilitates interoperable, real-time transfers between bank accounts and, indirectly, mobile wallet platforms. The regulatory design clearly delineates roles: while system operation is delegated to a private shareholding company, regulatory authority remains firmly vested in the CBJ, which approves operating rules, sets technical and security standards, and oversees systemic risk management. This arrangement reflects a regulatory priority on system integrity, reliability, and settlement finality, ensuring that instant payments function smoothly and securely across participating institutions. (Alrfoua et al., 2026)

From the perspective of financial crime governance, Jordan's approach is anchored in a combination of preventive regulation and criminal law enforcement. Preventively, the CBJ has issued extensive AML/CFT instructions applicable to banks and payment service providers, mandating customer due diligence, transaction record-keeping, sanctions screening, and ongoing monitoring of payment flows. These obligations extend to real-time transfers conducted via CliQ, with institutions required to identify and report suspicious transactions to the competent financial intelligence authorities. The traceability of instant payments is frequently emphasised by regulators and industry actors as a core safeguard, on the premise that the digital audit trail associated with each transaction enhances the detection of fraud and money laundering risks in line with international "know your customer" standards (Central Bank of Jordan, 2024). Additional regulatory instruments, such as CBJ circulars governing transaction fees and data reporting, further demonstrate the close supervisory attention paid to payment system operations. (Al-Own et al., 2025)

In systemic terms, this framework aligns closely with international best practices in payment system oversight and AML compliance. Jordan's payment infrastructures are subject to periodic assessments by international bodies, and there is little evidence of structural weaknesses in the technical operation of CliQ itself. However, this emphasis on prevention and system-level security is complemented—and, in some respects, overshadowed—by a strong reliance on criminalisation as the primary response to digital payment fraud. (Awaisheh et al., 2025a)

On the punitive side, Jordan has significantly strengthened its criminal law toolkit. The Cybercrime Law No. 17 of 2023 introduced explicit offences targeting online fraud, identity theft, phishing, and electronic payment scams, accompanied by increased penalties reflecting the seriousness of cyber-enabled financial crime. These provisions operate alongside general fraud offences under the Penal Code, enabling prosecution where deception results in the unlawful acquisition of funds. Moreover, Jordan's Anti-Money Laundering and Counter Terrorism Financing Law criminalises the knowing concealment, transfer, or conversion of illicit proceeds, thereby capturing conduct by fraudsters as well as third-party money mules who facilitate the laundering of scam-derived funds. In principle, courts may order restitution as part of criminal sentencing, and confiscation of criminal assets is available as an ancillary measure. Law enforcement authorities have reported a rise in cyber-fraud cases in recent years, a trend attributed to increased digitalisation, and the 2023 legislative reforms have been publicly framed as a necessary response to this evolving threat environment. (Rukba et al., 2025)

Despite the apparent robustness of this criminal and regulatory framework, a critical gap emerges when the analysis shifts from system protection and offender punishment to victim outcomes. Jordanian law does not provide a dedicated mechanism for compensating victims of fraud committed through instant payment systems. The governing assumption is that a payment executed via CliQ is final and irrevocable once settled, reflecting a

foundational principle of payment system law designed to preserve certainty and stability. Where a customer is deceived into authorising a transfer, the transaction is processed within seconds, and funds are typically credited to the recipient's account almost immediately. At that point, banks lack legal authority to reverse the transfer unilaterally without the recipient's consent, even where fraud is suspected (Al-Batoush, 2024).

Although some banks have introduced optional features allowing recipients to return funds in cases of error, such mechanisms are neither universal nor effective against intentional fraud, as scammers have no incentive to cooperate. Consequently, the victim's recourse is largely confined to reporting the incident to their bank and to law enforcement. While early intervention may result in the freezing of accounts in limited cases, recovery remains uncertain once funds are withdrawn or transferred onward. Civil law remedies, such as actions for unjust enrichment, offer only theoretical relief where the perpetrator is unidentified or judgment-proof. Crucially, under the prevailing legal framework, banks and payment service providers bear no general obligation to reimburse losses arising from authorised payment fraud. Absent demonstrable negligence on the part of the institution—such as a failure to comply with mandatory security or AML requirements—the loss is allocated to the individual who authorised the transfer. (Alhrerat et al., 2025)

This allocation of risk is consistent with the dominant regulatory narrative in Jordan, which portrays digital payment systems as fundamentally secure and frames fraud primarily as a consequence of user error or insufficient vigilance (Central Bank of Jordan, 2024). Public communications and industry initiatives reinforce this perspective through extensive awareness campaigns advising customers to protect credentials and resist social engineering attempts. The Association of Banks in Jordan, for example, has launched educational platforms and mobile applications aimed at improving consumer literacy in digital banking and fraud prevention. While such measures undoubtedly contribute to risk reduction, they also reflect a policy logic of responsibilisation, whereby individuals are positioned as the primary line of defence against fraud. (Abuanzeh & Alshayyab, 2025)

The practical implications of this model are evident in reported cases involving CliQ-related scams. Fraudsters have impersonated bank officials or service providers, persuading customers to initiate instant transfers under false pretences. Even where perpetrators are later apprehended and convicted, victims are not automatically reimbursed and remain dependent on the uncertain outcomes of criminal proceedings or asset recovery efforts. (Alayaydeh et al., 2025) In effect, the legal system prioritises deterrence and punishment over restitution, leaving victims exposed to potentially significant financial harm. (Al-Hunaiti, 2025)

In summary, Jordan's instant payment framework can be characterised as one of criminalisation without compensation. The system is tightly regulated to ensure operational security and AML compliance, and criminal law has been adapted to address cyber-enabled fraud. Yet the legal architecture stops short of reallocating losses or providing systematic redress to victims of authorised payment fraud. (Awaisheh, 2025a) As instant payments become increasingly embedded in everyday financial activity, this asymmetry raises fundamental questions about the sustainability and fairness of the current model. The Jordanian approach stands in contrast to emerging regulatory trends elsewhere, suggesting that reliance on criminalisation and user responsibility alone may prove insufficient if fraud incidents increase in frequency or sophistication.

Authorised Push Payment Fraud and the UK Regulatory Turn

The United Kingdom's response to authorised push payment (APP) fraud provides a revealing comparative contrast, illustrating how a legal system can evolve from a predominantly punitive and victim-responsibilising approach to a regulatory model grounded in systemic accountability and mandatory victim compensation. APP fraud in the UK encompasses a broad range of scam typologies in which victims are deceived into authorising payments to accounts controlled by fraudsters. These include impersonation scams involving false representations as banks or government agencies, romance and investment scams, and invoice fraud targeting both consumers and small businesses. What distinguishes APP fraud from unauthorised payment fraud is not the absence of harm or culpability, but the presence of formal authorisation: the victim authenticates and initiates the payment instruction, albeit under manipulation. This distinction proved legally decisive within the UK framework, where existing payment laws and consumer protection rules afforded strong reimbursement rights for unauthorised transactions but offered no equivalent protection to victims who had authorised transfers under false pretences (Payment Services Regulations 2017; Braithwaite, 2024).

As the use of real-time payments expanded, this regulatory asymmetry became increasingly untenable.

The Faster Payments system, introduced in 2008 to enhance efficiency and immediacy in retail banking, enabled near-instant settlement and high availability but also narrowed the window for fraud detection and intervention. Victims could be deceived by highly convincing social engineering techniques and see funds transferred, dispersed, and laundered within minutes. By the late 2010s, APP fraud had escalated sharply, with reported losses reaching hundreds of millions of pounds annually. UK Finance data indicated that APP fraud losses exceeded £580 million in 2021 alone, with subsequent years showing continued growth, a trend exacerbated during the COVID-19 pandemic as digital dependency increased and scammers exploited social isolation and economic anxiety (UK Finance, 2024; National Audit Office, 2023). The UK government's Fraud Strategy published in 2023 acknowledged fraud as the most prevalent crime in England and Wales and identified APP scams as a rapidly growing and particularly harmful subset, overtaking card fraud in both prevalence and consumer impact. (Almaaitah et al., 2025)

For an extended period, the UK's legal response to this phenomenon closely resembled the model observed in Jordan. Fraud was treated primarily as a matter of criminal wrongdoing and consumer vigilance, with losses generally falling on victims unless bank fault could be established. Banks consistently denied liability for APP losses on the basis that payments were properly authorised and authenticated, and this position was ultimately affirmed at the highest judicial level. In *Philipp v Barclays Bank UK plc* [2023] UKSC 25, the Supreme Court rejected the argument that banks owed a general duty to protect customers from the consequences of authorised payments induced by fraud. The Court confirmed that the so-called *Quincecare* duty—developed to protect corporate customers from dishonest agents—did not extend to situations where an individual customer personally authorised the payment. As a matter of existing law, banks were obliged to execute customer instructions promptly and were not required to assess the wisdom or underlying motivations of the customer's decision, even where deception was suspected (Barillà, 2024; Braithwaite, 2024).

The practical consequences of this doctrinal position were severe. Criminal investigations into APP fraud were frequently slow, complex, and transnational, with limited prospects of asset recovery once funds had been dissipated through mule accounts. Victims were often left bearing catastrophic financial losses with no enforceable right to reimbursement. This outcome prompted sustained criticism from consumer advocates, parliamentary committees, and regulators, who characterised the prevailing framework as placing an unrealistic and unfair burden on individuals confronted with increasingly sophisticated scams (Ngan, 2025). While education and awareness campaigns were expanded, it became clear that prevention alone could not address a problem that had acquired systemic dimensions. (Al-Mustarayhi et al., 2025)

In response, the UK initially pursued a series of voluntary and technological interventions. Banks implemented the Confirmation of Payee service to reduce misdirected payments by alerting customers when recipient details did not match account records. While beneficial, this measure proved insufficient to prevent many APP scams, particularly those involving convincing impersonation narratives. More significantly, the banking industry introduced the Contingent Reimbursement Model (CRM) Code in 2019, under which participating institutions committed to reimburse victims of APP fraud unless the customer had acted fraudulently or with gross negligence. The CRM Code represented a normative shift by recognising that many APP victims were not meaningfully at fault. Reimbursement rates improved among participating banks, yet the voluntary nature of the scheme resulted in uneven coverage and inconsistent application. Large segments of the market, including some major institutions and many fintech providers, remained outside the Code, and interpretations of key concepts such as "gross negligence" varied widely (Braithwaite, 2024).

By the early 2020s, policymakers concluded that voluntary arrangements were inadequate to address what had become a structural risk to the payment system. Legislative and regulatory intervention followed. The Financial Services and Markets Act 2023 granted the Payment Systems Regulator explicit powers to mandate reimbursement for APP fraud. Exercising this authority, the regulator introduced a compulsory reimbursement regime embedded within the Faster Payments scheme rules, scheduled to take effect in October 2024. The new framework applies to the vast majority of APP fraud cases, given that most such scams in the UK are executed via Faster Payments. Under the scheme, victims are entitled to full reimbursement by default within a defined timeframe, subject only to limited exceptions, most notably where the customer's gross negligence or complicity contributed to the loss (Payment Systems Regulator, 2023; Pay.UK, 2024).

A distinctive feature of the UK model lies in its approach to cost allocation. Rather than placing the entire

reimbursement burden on the sending bank, the regulator adopted a cost-sharing mechanism under which both the sending and receiving payment service providers typically bear responsibility, often on a 50/50 basis. This design reflects the recognition that fraud prevention opportunities exist at both ends of the transaction: sending institutions control customer interfaces and payment initiation, while receiving institutions are positioned to detect mule accounts and suspicious inflows. By distributing liability, the scheme seeks to align incentives across the payment chain and encourage investment in preventive controls without disproportionately penalising any single actor. (Awaisheh et al., 2025b)

The regulatory turn toward mandatory reimbursement represents a paradigmatic shift in the governance of instant payment fraud. Notably, the UK did not respond by expanding criminal offences or increasing penalties; fraud was already criminalised. Instead, it addressed the failure of existing legal frameworks to allocate losses in a manner consistent with the realities of real-time payments. By collectivising the risk of APP fraud and embedding compensation obligations within payment system rules, the UK reframed fraud losses as a systemic externality requiring regulatory correction. While concerns remain regarding potential moral hazard and cost pass-through to consumers, regulators have sought to mitigate these risks through the retention of fault-based exceptions, ongoing consumer education, and enhanced data reporting and transparency obligations. (Awaisheh et al., 2025c)

In sum, the UK's experience demonstrates that APP fraud in instant payment systems cannot be effectively managed through criminal law and consumer vigilance alone. The move toward mandatory reimbursement reflects an acknowledgment of market and regulatory failure in the original allocation of losses and marks a transition from individual responsibilisation to systemic accountability. This evolution provides a critical reference point for jurisdictions such as Jordan, where instant payment adoption is accelerating but where comparable mechanisms for victim protection and loss redistribution have yet to emerge.

Comparative Analysis: Jordan and the United Kingdom

A side-by-side examination of Jordan's and the United Kingdom's approaches to authorised push payment fraud reveals two distinct regulatory philosophies in the governance of financial crime within instant payment systems. While both jurisdictions acknowledge that real-time payments generate heightened risks of fraud and money laundering, they differ markedly in how those risks are conceptualised, allocated, and managed. (Al-Kasassbeh et al., 2024)

In Jordan, the dominant policy priority has been to foster trust in digital payments and encourage adoption by emphasising system security, reliability, and low reported fraud incidence. Official narratives consistently highlight that platforms such as CliQ are technically robust and that fraud losses remain minimal relative to overall transaction volumes. This framing implicitly treats fraud as an exception rather than an inherent feature of instant payments and reinforces the notion that adherence to user precautions and awareness campaigns is sufficient to maintain system safety. The United Kingdom, by contrast, reached a different assessment as its instant payment ecosystem matured. Confronted with sustained and escalating APP fraud losses, UK regulators increasingly acknowledged that even diligent and informed users could fall victim to sophisticated scams. As a result, policy attention shifted from prevention alone to impact mitigation, recognising that maintaining public confidence required institutional fail-safes capable of absorbing losses when fraud inevitably occurs. (Alhasan & Awaisheh, 2024)

The most pronounced divergence between the two systems concerns the legal position of the victim. Under Jordanian law, victims of authorised payment fraud have no guaranteed right to compensation from banks or payment service providers. Their legal relationship is primarily adversarial with respect to the fraudster, and redress is pursued through criminal investigation or, in theory, civil claims that are often impractical once funds have been dissipated. Financial institutions play a cooperative role by providing information or freezing accounts when possible, but they do not assume responsibility for compensating losses. In the United Kingdom, the introduction of mandatory reimbursement fundamentally altered this dynamic. Victims of APP fraud are now entitled, in most cases, to reimbursement from their bank, transforming the post-fraud relationship into one of institutional support rather than individual exposure. This shift provides UK consumers with a level of financial protection that is currently absent in the Jordanian framework. (Awaisheh & Al-Dabbas, 2024)

Closely related to this is the role assigned to payment service providers. In Jordan, PSPs are primarily

responsible for implementing preventive measures such as customer due diligence, authentication protocols, and transaction monitoring to comply with AML obligations and protect system integrity. Once an authorised payment is executed, however, their responsibility largely ends unless institutional fault can be demonstrated. In the UK's post-reform framework, PSP responsibilities extend beyond prevention to encompass outcome management. Banks are required not only to attempt to stop fraud ex ante through warnings and confirmation mechanisms, but also to reimburse customers when those measures fail. This regulatory obligation ensures that PSPs internalise at least part of the cost of fraud, thereby creating stronger incentives to invest in prevention, intervention, and intelligence-sharing. (Al-Zubi et al., 2024) By contrast, Jordanian PSPs do not internalise APP fraud losses in a comparable manner, as the financial burden remains with the victim unless recovery is achieved through enforcement.

These differences are reflected in the mechanisms for allocating fraud losses. Jordan lacks any formalised loss-allocation regime for authorised payment fraud. Losses remain individualised and are addressed, if at all, through case-by-case criminal restitution or civil claims. The UK, by contrast, has instituted a structured and rule-based loss-allocation mechanism embedded within the Faster Payments scheme. Under this model, losses are allocated primarily to the sending and receiving PSPs, typically on a shared basis, thereby spreading the cost of fraud across the financial sector rather than concentrating it on individual victims. In effect, this arrangement resembles a form of collective insurance against APP fraud, designed to stabilise consumer confidence in instant payments. (Awaisheh et al., 2024a)

The two systems also diverge in their treatment of evidentiary burdens and liability exceptions. In Jordan, the burden rests largely on the victim or the prosecuting authorities to establish fraud and identify the perpetrator, with institutional liability arising only in rare cases of demonstrable bank negligence. In the UK reimbursement regime, the default presumption operates in the opposite direction: reimbursement is owed unless the bank can demonstrate that a defined exception applies, most notably where the customer acted fraudulently or with gross negligence. This reversal of the burden of proof represents a significant recalibration of consumer protection, signalling that victims are entitled to redress unless clear evidence indicates otherwise. (Awaisheh et al., 2024b) Jordan's framework, by comparison, applies a far stricter implicit standard, under which even careful users deceived by sophisticated scams bear the loss.

Concerns about moral hazard further illuminate the contrasting policy choices. Jordan's approach minimises moral hazard by ensuring that users retain full financial responsibility for authorised payments, thereby maximising incentives for vigilance. The cost of this approach is the absence of meaningful protection for victims who act reasonably yet fall prey to fraud. The UK's model confronts moral hazard directly by coupling broad reimbursement rights with fault-based exceptions and continued emphasis on consumer education. By retaining a gross negligence standard and monitoring repeat behaviour, UK regulators seek to balance victim protection with incentives for caution, accepting a degree of risk-sharing as the price of fairness and trust in the payment system. (Awaisheh, 2023)

Both jurisdictions integrate AML controls into their instant payment frameworks, yet the interaction between AML and reimbursement differs in practice. Jordan relies heavily on AML measures to intercept suspicious flows and pursue offenders, and its strict AML laws and reporting obligations provide strong tools for criminal enforcement. However, these tools do little to alleviate harm once losses have occurred. In the UK, the mandatory reimbursement regime is expected to complement AML efforts by strengthening incentives for banks to prevent fraudulent transfers before completion and to enhance cooperation in identifying mule accounts and organised scam networks. The comparative experience suggests that reimbursement mechanisms need not undermine AML objectives; rather, they can reinforce them by aligning institutional incentives with proactive fraud disruption. (Dwan et al., 2023)

Taken together, Jordan and the United Kingdom illustrate two ends of a regulatory spectrum in addressing instant payment fraud. Jordan's model reflects a logic of responsibilisation, prioritising system security and individual vigilance while leaving loss allocation largely untouched. The UK's post-2024 framework embodies systemic accountability, recognising APP fraud as an inherent risk of instant payments that must be collectively managed to preserve fairness and trust. Each approach entails trade-offs: Jordan's limits institutional costs but externalises harm to victims, while the UK's redistributes losses across the financial sector with potential downstream effects on pricing and system design. (Al Atiyat et al., 2025) As instant payments continue to

expand, the comparative analysis suggests that pressure will mount on jurisdictions like Jordan to reconsider whether a purely criminalisation- and prevention-focused model remains sustainable in the face of increasingly sophisticated and persistent fraud.

Policy Implications and Reform Proposals for Jordan

The comparative analysis between Jordan and the United Kingdom carries significant policy implications for the future governance of instant payment systems in Jordan. It demonstrates that reliance on a purely crime-centred and victim-responsibility model, while effective in deterring and punishing offenders, leaves unresolved vulnerabilities in the broader resilience of the digital payments ecosystem. As Jordan continues its transition towards a cashless economy and further embeds platforms such as CliQ into everyday financial activity, the likelihood of more frequent and sophisticated fraud incidents will increase. The critical policy question is therefore not whether fraud will occur, but how the legal system should respond when preventive and criminal enforcement measures fail.

A central implication is the need to reconsider the current allocation of losses arising from authorised payment fraud. Jordan could move toward introducing a limited mandatory reimbursement framework for defined categories of digital payment fraud, calibrated carefully to local conditions. Such a scheme would not need to replicate the UK's full-scale model at the outset. Instead, it could initially apply only to individual consumers, exclude business accounts, and impose transaction value caps to manage exposure and assess behavioural effects. Reimbursement would be conditional, available only where the customer has not acted fraudulently or with gross negligence, thereby preserving incentives for basic vigilance. This approach mirrors the UK's "consumer standard of caution" while avoiding the moral hazard associated with unconditional guarantees. The policy rationale is straightforward: ensuring that ordinary users who act reasonably are not left to absorb catastrophic losses that can undermine confidence in digital payments more broadly. From an institutional perspective, such a framework could initially be implemented through a CBJ-endorsed industry code and later formalised through binding regulation once operational experience is gained. (Al Atiyat et al., 2024)

Closely connected to this is the question of cost allocation. Any reimbursement regime in Jordan should avoid concentrating the financial burden on a single institution. A shared-liability model, whereby both the sending and receiving payment service providers contribute to reimbursement, would better align incentives across the payment chain. This reflects the reality that fraud prevention opportunities exist at both ends of an instant payment transaction: the sending institution controls customer interfaces and warnings, while the receiving institution is best placed to identify mule accounts and suspicious inflows. JoPACC and the CBJ could facilitate this arrangement by establishing inter-institutional settlement rules or a central reimbursement mechanism embedded within CliQ's operating framework. Proportional contributions, insurance arrangements, or risk-based adjustments could be used to accommodate smaller providers, ensuring that the scheme enhances collective responsibility without distorting competition.

Another important reform area concerns intervention powers and timing. Jordan's current emphasis on instantaneity can constrain banks' ability to intervene once fraud indicators emerge. Regulatory clarification could empower payment service providers to introduce limited, proportionate delays for high-risk transactions, allowing additional verification where algorithmic or behavioural flags are triggered. The experience of other jurisdictions shows that introducing targeted friction does not undermine the overall efficiency of instant payments when applied narrowly and transparently. Measures such as a Confirmation of Payee service within CliQ, combined with a clearer legal mandate to pause or warn in suspicious cases, would strengthen banks' ability to act in customers' interests while remaining consistent with settlement finality principles.

Crucially, any shift toward reimbursement must be explicitly decoupled from leniency toward offenders. Strengthening victim protection should not dilute Jordan's commitment to criminal enforcement and anti-money laundering. On the contrary, reimbursement can coexist with, and even reinforce, aggressive pursuit of fraudsters. Banks or collective reimbursement mechanisms could be subrogated to victims' recovery rights, enabling them to pursue restitution once perpetrators are identified. Confiscated assets and proceeds recovered through AML enforcement could be used to offset reimbursement costs. This two-track approach—immediate victim relief combined with uncompromising criminal prosecution—ensures that the burden of enforcement

does not fall on victims while maintaining deterrence against fraud and laundering activities.

The analysis also points to the importance of cross-sector collaboration. Instant payment fraud rarely originates solely within the banking system; it often relies on telecommunications networks, digital advertising, and online platforms to reach victims. Jordan could enhance coordination between financial institutions, telecom operators, and digital platforms through formal information-sharing arrangements and joint task forces led by the CBJ or a specialised financial crime unit. Measures such as blocking spoofed calls, filtering scam messages, and monitoring fraudulent online advertisements would complement payment system reforms and reflect a "whole-of-system" approach to financial crime governance.

Given the scale and novelty of these reforms, gradual implementation supported by data monitoring is essential. Jordan could pilot reimbursement obligations for specific scam typologies or limited time periods, collecting detailed data on fraud incidence, reimbursement costs, recovery rates, and behavioural responses. Transparent reporting by banks to the CBJ on how fraud cases are handled would support evidence-based refinement of the framework. Over time, such data would allow regulators to assess whether concerns about moral hazard materialise and whether the benefits in consumer trust and system resilience justify expansion of the scheme.

Finally, consumer education remains a necessary complement to institutional reform. Even with compensation mechanisms in place, sustained financial literacy initiatives are essential to promote a culture of caution. Public messaging should make clear that reimbursement is conditional and that reckless behaviour may disqualify claims. Framing reforms as a shared effort between regulators, banks, and users—rather than as a blanket safety net—helps preserve deterrence and avoids signalling impunity to fraudsters. Jordan's existing awareness campaigns provide a strong foundation for embedding this balanced narrative.

Taken together, these proposals suggest a measured yet proactive reform trajectory. While Jordan's banking sector is smaller and current reported fraud levels are lower than those observed in the UK, comparative experience indicates that instant payment infrastructures inevitably attract criminal adaptation as they mature. Building compensatory and risk-sharing mechanisms at an early stage is therefore a strategic investment in the sustainability of digital finance. By adopting a limited, carefully designed reimbursement framework alongside robust enforcement and prevention, Jordan can ensure that the benefits of instant payments—speed, convenience, and inclusion—are not eroded by unchecked fraud, and that the legal system evolves in step with technological innovation.

Conclusion

The expansion of instant payment systems such as the United Kingdom's Faster Payments and Jordan's CliQ illustrates the dual nature of contemporary digital finance: unprecedented speed and efficiency on the one hand, and heightened exposure to financial crime on the other. This article has demonstrated that the legal challenges posed by authorised push payment (APP) fraud and related money laundering cannot be adequately addressed through traditional criminalisation strategies or compliance-oriented anti-money laundering frameworks alone. Instead, they require a re-examination of how legal systems allocate risk and loss within payment infrastructures that are designed to prioritise immediacy and finality.

The comparative analysis highlights a fundamental divergence in regulatory philosophy. The United Kingdom's response to escalating APP fraud reflects a recognition that such fraud constitutes a structural risk inherent in real-time payment systems rather than a mere aggregation of individual lapses. By mandating reimbursement for scam victims and redistributing losses across payment service providers, the UK has moved beyond a model centred on victim responsibility and post hoc punishment. This regulatory turn acknowledges that even cautious and informed users can be deceived by sophisticated scams and that systemic trust in instant payments depends on collective mechanisms for absorbing harm (Braithwaite, 2024; Payment Systems Regulator, 2023). Importantly, this shift did not entail expanding criminal offences or weakening enforcement; rather, it complemented criminal law by addressing its limits in restoring victims to their pre-offence position.

Jordan's current framework presents a contrasting picture. Significant progress has been made in modernising payment infrastructure, strengthening AML controls, and criminalising cyber-enabled fraud. These measures have contributed to a secure and growing digital payments ecosystem. Yet the absence of any structured compensation mechanism for victims of authorised payment fraud exposes a legal design gap. The

prevailing model prioritises system integrity and offender punishment but leaves individuals to bear losses once fraud occurs, effectively externalising the cost of systemic vulnerabilities onto users. While this approach may appear sustainable in a low-fraud environment, comparative experience suggests that it becomes increasingly fragile as instant payments mature and criminal techniques evolve.

The core contribution of this article lies in reframing financial crime in instant payment systems as a problem of legal and institutional design, not merely one of criminal behaviour or user negligence. APP fraud illustrates how the combination of speed, irrevocability, and social engineering can overwhelm both individual vigilance and ex post enforcement. The UK's regulatory evolution demonstrates that loss allocation is not a peripheral issue but a central component of effective financial crime governance in real-time payment systems. By contrast, Jordan remains at a crossroads: it can maintain a model of pure criminalisation and responsibilisation, or it can proactively integrate compensatory and accountability mechanisms informed by comparative experience.

The policy implications are clear. A calibrated reimbursement framework—limited in scope, conditional on the absence of gross negligence, and supported by shared liability among payment service providers—offers a viable middle ground. Such an approach would enhance consumer protection without undermining payment finality, AML enforcement, or deterrence. It would also align legal incentives with the realities of instant payments, encouraging institutions to invest in prevention and intervention while preserving public confidence in digital finance. Importantly, providing compensation to victims should not be misconstrued as leniency toward fraudsters; it represents a decoupling of victim relief from the uncertain outcomes of criminal prosecution, allowing both objectives to be pursued simultaneously.

More broadly, this study contributes to an emerging shift in how fast payment systems are regulated globally. As more jurisdictions adopt real-time payments, the policy debate is likely to move beyond questions of detection and punishment toward questions of resilience, fairness, and trust. The traditional sequence of "crime followed by punishment" often fails to deliver timely justice for victims in a digital context where losses are immediate and recovery is uncertain. The emerging model—"crime, compensation, then accountability"—offers a more holistic legal response, one that recognises the shared responsibility of users, institutions, and regulators in managing systemic risk.

In conclusion, financial fraud and money laundering in instant payment systems should be understood not simply as the actions of bad actors, but as stress tests of the legal frameworks governing modern finance. Jordan's and the United Kingdom's experiences, though shaped by different institutional contexts, underscore a common lesson: effective responses to digital financial crime require legal innovation that keeps pace with technological change. Designing payment systems that are not only fast and efficient, but also fair and resilient, demands collective solutions that integrate criminal justice, regulatory policy, and consumer protection. As instant payments become the default mode of financial exchange, the ability of legal systems to distribute risk justly will be central to sustaining trust, inclusion, and the rule of law in the digital economy.

References

Abuanzeh, A., & Alshayyab, L. (2025). The legal concept of excessive usury on sale and lending and the liability arising therefrom in the Jordanian criminal law and civil law: A comparative study with French law. Jordanian Journal of Law and Political Science, 17(3). https://doi.org/10.35682/jjlps.v17i3.1182

Al-Atiyat, M., Aldweri, K., & Alsoud, A. R. (2024). International trade law and the World Trade Organization: Promoting global economic cooperation. Journal of Ecohumanism, 3(3). https://doi.org/10.62754/joe.v3i3.3402

Al-Atiyat, M., Aldweri, K., & Alsoud, A. R. (2025). Investor-state dispute settlement mechanisms in international trade. European Business Law Review. https://doi.org/10.54648/eulr2025029

Al-Batoush, B. M. (2024). CliQ transfers and legal remedies for erroneous or fraudulent payments. Jordan Pulse. https://jordanianlaw.com

Al-Hunaiti, M. (2025). Civil liability of the physician arising from medical errors in the Jordanian law. Jordanian Journal of Law and Political Science, 17(3). https://doi.org/10.35682/jjlps.v17i3.1134

Al-Kasassbeh, F. Y., Awaisheh, S. M., & Odeibat, M. A. (2024). Digital human rights in Jordanian legislation and international agreements. International Journal of Cyber Criminology. https://doi.org/10.5281/zenodo.4766803

Al-Mustarayhi, A., Khasawneh, M., & Qtaishat, A. (2025). The legal connection between actual damage and the value of the contractual indemnity: A comparative study between the Jordanian and Egyptian civil laws. Jordanian Journal of Law and Political Science, 17(3). https://doi.org/10.35682/jjlps.v17i3.1200

Al-Own, G., Al-Ou'n, A., & Alsarhan, M. (2025). The legal foundation of criminal responsibility of AI-enabled crimes according to the Jordanian law: Analytical study. Jordanian Journal of Law and Political Science, 17(4). https://doi.org/10.35682/jjlps.v17i4.1655

Al-Zubi, J. K., Maaqqbeh, M., Awaisheh, S. M., & Mofleh, M. (2024). Progress and challenges in the legal framework of women's rights in Jordan. International Journal of Criminal Justice Sciences. https://doi.org/10.5281/zenodo.19128

Alayaydeh, H. A., Awaisheh, S. M., Al-Taani, M., Al-Dabbas, N. A., Alqudah, A. M.-A., & Awaisheh, S. M. (2025). The problem of establishing civil liability for harmful effects of smart robots. Indian Journal of Information Sources and Services, 15(4), 31–39. https://doi.org/10.51983/ijiss-2025.IJISS.15.4.04

Alhasan, T. K., & Awaisheh, S. M. (2024). The right of public employees to defend disciplinary penalties in Jordan. International Journal of Public Law and Policy. https://doi.org/10.1504/IJPLAP.2024.137783

Alhrerat, K. A., Alnsour, T. M. Q., Almasarweh, S. I. M., Alqudah, A. M.-A., Awaisheh, S. M. A., & Awaisheh, S. M. (2025). Safeguarding electronic signatures in Jordan: Legal foundations and enforcement challenges. Indian Journal of Information Sources and Services, 15(4), 302–308. https://doi.org/10.51983/ijiss-2025.IJISS.15.4.34

Almaaitah, S., Al-Rahahla, R., & Al-Batoush, A. (2025). Compensation for damage in civil liability for stem cell banks in Jordanian legislation. Jordanian Journal of Law and Political Science, 17(3). https://doi.org/10.35682/jjlps.v17i3.1089

Alrfoua, A. Y., Awaisheh, S. M. A., Al-Wreikat, E. I., Al-Khraisat, W. M. M., Awaisheh, S. M., & Abdelrahman, A. (2026). The role of administrative regulatory authorities in protecting the environmental sustainability of natural resources: A legal analytical study. Scientific Culture, 12(1-1), 1–9. https://doi.org/10.5281/zenodo.11425133

Association of Banks in Jordan. (2024). Digital banking awareness and fraud prevention platform. https://www.abj.org.jo

Awaisheh, S. M. (2023). Digital justice in Jordan: The role of virtual arbitration sessions in modernizing the legal system. International Journal of Cyber Criminology. https://doi.org/10.5281/zenodo.4766609

Awaisheh, S. M. (2025a). From paper to pixels: The legal status and challenges of electronic writing in administrative contracts—A comparative study. Electronic Government. https://doi.org/10.1504/EG.2025.144726

Awaisheh, S. M., & Al-Dabbas, N. A. (2024). The dichotomy of interests: A comparative analysis of civil and administrative lawsuits in the Jordanian legal system. International Journal of Criminal Justice Sciences. https://doi.org/10.5281/zenodo.19108

Awaisheh, S. M., Al-Abbadi, H. S., Al-Dabbas, N. A., Hmaidan, R. M., Al-Khalaileh, L., & Al-Tarawneh, A. S.

(2025). New claims and causes of action before the court of appeal in Jordanian civil procedure. Journal of Human Security. https://doi.org/10.12924/johs2025.210108
Awaisheh, S. M., Alkhamaiseh, M. A., Al-Maagbeh, M. M., & Khalaileh, L. (2024). Artificial intelligence and its impact on administrative decision-making. Journal of Human Security. https://doi.org/10.12924/johs2024.20114
Awaisheh, S. M., Alsaraireh, N., Alkasasbeh, A. A. M., & Odeibat, M. A. (2025). The extent to which recourse to arbitration is permissible in the settlement of procurement contract disputes. Journal of Human Security. https://doi.org/10.12924/johs2025.210103
Awaisheh, S. M., Awaisheh, S. M., Abdelrahman, A., & Al-Thnaibat, O. H. A. (2025b). Environmental governance and administrative judiciary in Jordan and France: A socio-legal comparative study. International Journal of Sustainable Development and Planning, 20(12), 5491–5501. https://doi.org/10.18280/ijsdp.201238
Awaisheh, S., Al-Hassan, T., & Mansour, A. (2024). The status of digital evidence in administrative litigation. Al-Balqa Journal for Research and Studies, 27(3), 42–55. https://doi.org/10.35875/pgdx2798
Bank for International Settlements. (2021). Sound practices: Implications of fintech developments for banks and bank supervisors. https://www.bis.org
Barillà, S. (2024). Authorised push payment fraud and the limits of private law remedies. Journal of Banking Regulation, 25(2), 145–162.
Bello, A., Laxman, S., & Kumar, R. (2025). AI-based fraud detection in instant payment systems: Regulatory challenges. Computer Law & Security Review, 52, 105907. https://doi.org/10.1016/j.clsr.2024.105907
Braithwaite, J. (2024). From consumer responsibility to systemic accountability: Reframing APP fraud. Journal of Financial Crime, 31(1), 1–18. https://doi.org/10.1108/JFC-09-2023-0204
Central Bank of Jordan. (2016). Central Bank of Jordan Law No. 23 of 1971, as amended. https://www.cbj.gov.jo
Central Bank of Jordan. (2017). Electronic payment and money transfer bylaw No. 111 of 2017. https://www.cbj.gov.jo
Central Bank of Jordan. (2020). Circular on electronic transfer fees and reporting requirements. https://www.cbj.gov.jo
Central Bank of Jordan. (2022). National strategy for financial inclusion and digital payments. https://www.cbj.gov.jo
Central Bank of Jordan. (2024). Annual report and payment systems statistics. https://www.cbj.gov.jo
Dwan, N., Aljazi, J. D., & Alsweilmieen, S. (2023). Analysis of recent civil service provisions vs. university employee systems in Jordan: Issues and solutions. Information Sciences Letters, 12(7), 2975–2982. https://digitalcommons.aaru.edu.jo/isl/vol12/iss7/24
European Central Bank. (2019). Card fraud statistics and payment security. https://www.ecb.europa.eu
Financial Services and Markets Act 2023 (UK). https://www.legislation.gov.uk
Górka, J. (2025). Instant payments and financial crime risk: A comparative perspective. Cambridge University Press. https://doi.org/10.1017/9781009059207
Hartmann, M., Straub, S., & Welte, A. (2019). Retail payments and financial stability. Journal of Financial Market Infrastructures, 7(3), 1–27. https://doi.org/10.21314/JFMI.2019.097
HM Government. (2023). Fraud strategy. https://www.gov.uk
JoPACC. (2023). CliQ operating rules and system overview. https://www.jopacc.com
Jordan. (2007). Anti-money laundering and counter terrorism financing law. https://www.cbj.gov.jo
Jordan. (2023). Cybercrime Law No. 17 of 2023. https://www.pm.gov.jo
Jordan News. (2024). Citizens fall victim to financial fraud: Urgent calls to safeguard personal data. https://www.jordannews.jo
McKinsey & Company. (2022). Managing financial crime risk in digital payments. https://www.mckinsey.com
National Audit Office. (2023). Tackling fraud and error in government. https://www.nao.org.uk
Ngan, C. (2025). Social engineering and authorised push payment fraud. Journal of Financial Crime, 32(2), 215–233. https://doi.org/10.1108/JFC-10-2024-0223
Pay.UK. (2024). Faster payments scheme rules—Mandatory reimbursement. https://www.wearepay.uk
Payment Services Regulations 2017 (UK). https://www.legislation.gov.uk

Payment Systems Regulator. (2023). Authorised push payment fraud reimbursement requirement. https://www.psr.org.uk

Philipp v Barclays Bank UK plc [2023] UKSC 25. https://www.supremecourt.uk

Rukba, R. O. A., Awaisheh, S. M. A., Al-Hobabseh, W. I., Al-Khalaileh, L., Hmaidan, R. M., Althunibat, A. O., Awaisheh, S. M., & Abdelrahman, A. (2025). Balancing efficiency and ethics in public administration: The role of artificial intelligence in administrative law of the Middle East. Research Journal in Advanced Humanities, 6(4). https://doi.org/10.58256/ktbmht44

UK Finance. (2024). Fraud the facts 2024. https://www.ukfinance.org.uk

World Bank. (2022). Financial consumer protection and fraud risks in digital payments. https://www.worldbank.org