Buna–FNA Working Paper

Countering Cross-Border Fraud and Scams in Arab Countries

Samira Neaimeh
Buna

Dr Kimmo Soramäki
FNA

Matteo Neri
FNA

October 2026



Executive Summary 3
1. Introduction 4
2. The Evolving Fraud Landscape in the Arab Region 6
3. National Responses: National Anti-Scam Utilities 7
3.1 Malaysia: Central Bank and FMI as Partners in National Fraud Response 8
3.2 Other National Approaches 9
3.3 Impact of National Anti-Scam Utilities 10
4. The Cross-Border Challenge 11
4.1 FATF and MENAFATF Recommendations on Information Sharing 11
4.2 The Cross-Border Limits of National Utilities 12
4.3 Cross-Border Intelligence Sharing in Practice 12
4.4 Law Enforcement Coordination 12
5. Tools for Cross-Border Fraud Resilience 13
5.1 Cross-Border Track and Trace 13
5.2 Cross-Border Secure Exchange of Fraud Intelligence 14
5.3 Cross-Border Consumer Case Transparency and Scam Report Intelligence 15
5.4 Privacy-Preserving Identity Exchange 15
6. Exploring Buna's Potential Role in Regional Fraud Resilience 16
6.1 Buna's Legal Foundation and Objectives 16
6.2 Buna's Existing Capabilities 16
6.3 The FMI Model: From PayNet to Buna 17
6.4 National Anti-Scam Utility Integration with Buna's Settlement Layer 17
6.5 The Potential Value of a Regional Coordination Layer 18
6.6 Sovereignty, Security, and Strategic Resilience 19
6.7 Interoperability with Other Regional Hubs 19
7. Conclusion 20
Bibliography 21

Executive Summary

Arab countries have made significant investments in modernising their financial infrastructure. Buna, the cross-border payment platform established by the Arab Monetary Fund (AMF) as an international organisation, facilitates cross-border payment clearing and settlement across Arab and international currencies. Governments across the region have also developed regulatory frameworks, financial intelligence capabilities, and consumer protection mechanisms.

However, as payments become faster and more interoperable, fraud and scam typologies have rapidly adapted, exploiting systemic gaps across national boundaries. The fragmentation of fraud detection systems, which are often limited to domestic visibility, has created vulnerabilities that organised criminal networks increasingly exploit through sophisticated cross-border laundering schemes. In a global environment where payment infrastructure is increasingly recognised as critical to national security and economic sovereignty, the ability to detect, trace, and disrupt illicit financial flows is not merely a consumer protection function. It is a core component of a country's sovereign control over its financial system.

A growing number of countries have responded by establishing National Anti-Scam Utilities (NASUs). The capability they provide is a prerequisite for maintaining consumer trust, financial system integrity, and sovereign oversight of payment flows. A central premise of this paper is that effective cross-border fraud response depends on these domestic capabilities being in place first. A regional coordination layer can only be as strong as the national systems it connects. The Malaysian model, where Bank Negara Malaysia and PayNet partner to operate the National Fraud Portal, demonstrates that a central bank financial market infrastructure (FMI) partnership can serve as one institutional arrangement for coordinated fraud response, a model with direct relevance to the Arab region.

This paper covers one part of the anti-fraud effort. It looks at how financial and payment infrastructure can detect, trace and intercept fraudulent transactions after they have been made, and at the coordination this needs across borders. This paper explores the cross-border fraud challenge facing the Arab region, reviews international experience, and examines a range of options for strengthening regional fraud resilience. For jurisdictions that have not yet established national anti-fraud coordination capabilities, it presents the evidence for why such a capability is becoming necessary. For those that have, it examines how cross-border cooperation could extend their domestic effectiveness. The paper also considers what role a regional FMI, and Buna in particular, might play in facilitating cross-border fraud intelligence sharing and fund tracing as countries in the Arab region develop their national capabilities.

The authors invite central banks, financial institutions, and payment system operators across the Arab region to consider the options presented in this paper and to engage in further dialogue on how fraud resilience might be embedded within existing cross-border payment infrastructure.

1. Introduction

Arab countries stand at a critical juncture in the evolution of their financial infrastructure. Over the past two decades, Arab countries have invested significantly in modernising their payment systems and deepening regional economic integration. Domestic instant payment systems have been launched or are under development across the region, from the GCC to North Africa and the Levant. The establishment of Buna by the AMF, which now serves over 100 financial institutions across the Arab region and offers settlement in 7 currencies, represents a further advance in connecting Arab economies through modern, efficient payment channels.

Yet as the region's financial infrastructure matures, a new category of systemic risk has emerged: cross-border fraud and scams that exploit the very speed and interconnectedness that make modern payment systems effective. In a global environment where payment infrastructure is increasingly recognised as a matter of national security and economic sovereignty, the ability to detect, trace, and disrupt illicit financial flows is a core component of a country's sovereign control over its financial system. The AMF's Fintech Strategy Guidelines (AMF, 2020) and Cyber Resilience Oversight Guidelines (AMF, 2019) have already identified fraud, cybersecurity, and consumer protection as strategic priorities; this paper builds on that foundation.

Drawing on international case studies, regulatory developments, and the practical experience of deploying national-level fraud response systems, this paper examines the cross-border fraud challenge and explores options for how Arab countries could build a coordinated framework for regional fraud resilience. For jurisdictions that have not yet established national anti-fraud coordination capabilities, it presents the case for why such a capability is becoming essential. For those that have, it explores how cross-border cooperation could extend their domestic effectiveness. It is intended as a contribution to an ongoing discussion, not as a definitive proposal.

Countering fraud and scams involves four kinds of work. Prevention covers consumer awareness, authentication, and controls at the point of payment. Disruption covers action against the telephone networks, digital platforms and advertising channels criminals use to contact victims. Response covers the detection, tracing, freezing and recovery of funds after a fraudulent payment has left the victim's account. Enforcement covers investigation and prosecution. Prevention and disruption matter a great deal. They involve sectors well beyond finance, and they determine the number of cases that require a response at all. No jurisdiction can trace its way out of fraud. This paper addresses the response stage, and within it the contribution of financial and payment infrastructure and the coordination this requires across borders. It refers to the other three where they affect that stage.

This paper draws on three bodies of work, each of which addresses part of the cross-border fraud response challenge. The first is the policy literature on information sharing against financial crime, including the FATF standards on private-sector information sharing (Financial Action Task Force, 2017a, 2017b), the Egmont Group's principles for cooperation between financial intelligence units (Egmont Group, 2025), and studies of public-private partnerships (El Murr et al., 2023; Vogel, 2022; Asian Development Bank, 2024). It establishes the legal and institutional channels through which intelligence can be exchanged, although these typically operate over days or weeks. The second is work on cross-border payment infrastructure and privacy-preserving analytics. The CPMI, together with the IMF and the World Bank, has examined regional multilateral platforms for cross-border

payments, Buna among them (BIS CPMI, IMF & World Bank, 2023), while the BIS Innovation Hub's Project Aurora and SWIFT's recent experiments have shown that institutions can detect suspicious activity jointly without pooling their data (BIS Innovation Hub, 2023; SWIFT, 2025). These remain technical pilots, however, and leave open who may act on a result, on what legal basis, and with what liability. The third is the growing body of evidence on industrialised scam operations and payment fraud (UNODC, 2025; Interpol, 2025; EBA & ECB, 2024), which shows how much of the problem now crosses borders, beyond the reach of national arrangements.

The authors are not aware of work that examines the settlement layer of a regional financial market infrastructure as a point of fraud response, even though such an infrastructure observes the cross-border leg of a payment before it becomes final, and its rules already define the rights and liabilities of the institutions it connects. Work specific to the Arab region is also limited: the joint CPMI and AMF review of cross-border payments in AMF member countries refers to financial crime compliance only as a support to the regional payments agenda (BIS CPMI & AMF, 2024). The paper therefore asks one question: what institutional and technical arrangements would allow Arab jurisdictions to detect, trace and freeze fraudulent funds as they cross borders at the speed of instant payments, and what role could a regional financial market infrastructure such as Buna play in them? It answers three subsidiary questions. What national coordination capability is a prerequisite for cross-border response? Which cross-border mechanisms for intelligence sharing and fund tracing have proved effective elsewhere, and under what conditions? Which of them could build on Buna's existing connectivity, rules and governance, and what would need to be decided first? The question bears directly on the AMF's mandate for financial stability and regional financial integration, and on Buna's objectives set out in Section 6.1.

The paper takes the form of a comparative institutional analysis, in which each subsidiary question draws on its own body of evidence. For the first, Section 3 is built around Malaysia as the lead case. Malaysia offers the most fully documented example of the arrangement the paper examines, in which the central bank sets the strategic direction and the financial market infrastructure that operates the instant payment rails also operates the fraud response platform. This configuration is also the closest to that of the Arab region, where central banks operate or oversee the national payment systems. Indonesia illustrates a different route to the same capability, combining a response centre led by the financial services supervisor with fraud controls developed by the central bank in its instant payment system. The United Arab Emirates and three further Arab jurisdictions, anonymised because their initiatives are not yet public, indicate the region's starting points; none has yet reported results, and the three anonymised jurisdictions are described in the text only. Table 1 compares Malaysia, Indonesia, and the United Arab Emirates along four dimensions: governance and legal mandate, operating model and connection to payment rails, data-sharing arrangements, and reported results. For the second question, Section 4 reviews cross-border arrangements that are operating, have been piloted, or have been formally announced across several jurisdictions, distinguishing intelligence sharing between financial institutions and financial intelligence units from law enforcement coordination, and Section 5 sets out the tools on which the intelligence layer could build. For the third, Section 6 tests these findings against Buna's legal status, its rules and procedures, and its existing screening capability.

The analysis in Sections 3 to 6 relies primarily on official publications of central banks, payment system operators, standard setters, and international organisations, with press reports used to record

announcements, and is supplemented by the authors' practical experience of deploying national-level fraud response systems. Section 2, which sets out the context, also draws on industry surveys and press reports. Two of the authors work for FNA, which provided technology underpinning Malaysia's National Fraud Portal. Reported results are presented as published. Since they are reported by the authorities and operators concerned and are not collected on a consistent basis across jurisdictions, they should be read as indicative rather than strictly comparable.

The paper is structured as follows. Section 2 presents the evolving fraud landscape, with particular attention to the Arab region. Section 3 reviews national-level responses, including the emergence of National Anti-Scam Utilities, noting that in the Arab region these initiatives are being led by central banks, which in many cases also operate the national payment systems. Section 4 examines the cross-border gap that limits the effectiveness of national approaches. Section 5 outlines the technical and institutional tools available for cross-border fraud resilience, including consumer-facing case transparency and cross-border scam report intelligence. Section 6 discusses Buna's existing capabilities, including its current compliance and fraud screening mechanisms, and explores how similar constructions could serve as a foundation for more advanced cross-border fraud coordination. Section 7 concludes.

2. The Evolving Fraud Landscape in the Arab Region

Over the past decade, the global payments landscape has been transformed by innovations that have made transfers faster, cheaper, and more accessible. Instant payments, cross-border fast payment systems, and new forms of digital money have enabled unprecedented economic opportunities. Yet these same innovations have been rapidly exploited by transnational criminal organisations. Fraud and scams have become systemic risks, exploiting the fragmentation of anti-fraud measures within and across jurisdictions and the lack of effective mechanisms to monitor or intercept local cross-bank, cross-rail and cross-border financial crime.

The Arab region is not immune to these trends. In a survey by the UAE Government's Cybersecurity Council, 27% of respondents reported losing money to scams, with an average loss of US$2,194; only 9% fully recovered their losses (Emirates News Agency, 2024). Between 2021 and 2023, the UAE Financial Intelligence Unit estimated organised financial fraud losses at AED 1.2 billion, approximately USD 330 million (UAE Financial Intelligence Unit, 2024). Industry research on the true cost of fraud found that businesses in the UAE incur an average cost of AED 4.19 for every dirham lost to fraud, encompassing direct financial losses, internal costs, external fees, labour, and reputational damage (LexisNexis Risk Solutions, 2024).

A joint BIS CPMI and AMF analysis of cross-border payment developments across AMF member countries found that policymakers have set out an ambitious agenda to enhance intraregional payments, supported by improved financial crime compliance and payment system oversight (BIS CPMI & AMF, 2024). The challenge, however, extends well beyond the UAE. In Saudi Arabia, authorities have dismantled large-scale phishing and impersonation networks, including hundreds of fraudulent recruitment websites and spoofed digital payment portals (Al Arabiya English, 2022). The Saudi Central Bank (SAMA) has responded with a Counter-Fraud Framework for the institutions it supervises, which also requires them to run fraud awareness programmes (Saudi Central Bank, 2022).

In Egypt, the Central Bank convened its first Egypt Fraud Combating Forum in September 2024 (Central Bank of Egypt, 2024). Kuwait and other Gulf states have also experienced severe investment and cryptocurrency-related frauds, with individual cases involving losses in the tens of millions of dollars (Gulf News, 2024). Across the broader Europe, Middle East and Africa region, payments fraud losses were estimated at USD 94 billion in 2023 (Nasdaq Verafin, 2024), underscoring the global scale of the challenge.

The threat is also organisational. Fraud has been industrialised through dedicated scam centres, originally concentrated in Southeast Asia, where the combined cybercriminal labour force across Cambodia, Myanmar, and Laos is estimated to exceed 350,000 people, generating annual revenues of USD 50–75 billion (UNODC, 2025). These operations are now spreading globally. Interpol reports that scam centres have been identified across at least 25 countries, with the Middle East, West Africa, and Central America emerging as new areas of activity (Interpol, 2025). Victims from 66 countries have been trafficked into scam operations, and trafficking routes transiting through the Gulf region have been documented, with individuals recruited under false employment pretences before being diverted to fraud compounds (Interpol, 2025). The Global Initiative Against Transnational Organized Crime has noted that criminal groups are fragmenting into smaller, more mobile units and relocating operations to exploit weak governance environments worldwide (Amerhauser and Goodwin, 2026*)*. These findings underscore that fraud is no longer the province of opportunistic individuals but of organised transnational enterprises whose operations increasingly intersect with the Arab region.

These trends are accelerating. The Global Anti-Scam Alliance (GASA) estimates that consumers worldwide lost over USD 1 trillion to scams in 2024 (GASA, 2024). Reports of generative AI-enabled scams rose by 456 per cent between May 2024 and April 2025 (TRM Labs, 2025), while deepfake fraud attempts rose by more than 1,300 per cent in 2024 (Pindrop, 2025). The United Kingdom illustrates the enforcement gap: fraud accounts for over 40 per cent of all crime in England and Wales but receives less than 1 per cent of police resource, and over 70 per cent either originates abroad or has an international element (UK Home Office, 2023). A consistent cross-border pattern has emerged: the initial fraudulent transaction is typically domestic, while the second and third hops move funds across borders, beyond the reach of any single national authority. Fraud is not an isolated consumer protection issue but a systemic risk. A financial system that cannot trace illicit flows, freeze stolen funds, or identify mule networks is structurally incomplete as sovereign infrastructure.

3. National Responses: National Anti-Scam Utilities

In recent years, several jurisdictions have recognised that fraud and scams cannot be addressed effectively solely through institution-level initiatives. National Anti-Scam Utilities (NASUs) have emerged as a new layer of national infrastructure, centralising fraud and scam response at the country level. Several jurisdictions use the label Anti-Scam Centre, but that term covers different functions in different countries. This paper uses National Anti-Scam Utility to describe the capability rather than any one institutional form. A NASU can be operated by a central bank, by a financial market infrastructure under central bank oversight, by a consortium owned by the banks, or under a federated arrangement in which institutions keep their own systems and connect through common standards. The choice depends on a jurisdiction's legal mandate for data sharing, the coverage and connectivity of its payment infrastructure, and which institution has the capacity to operate it. By

creating a shared utility that integrates banks, payment operators, financial intelligence units, law enforcement agencies, and central banks, NASUs enable real-time collaboration across the financial ecosystem. Their defining feature is the ability to provide a common, automated environment for reporting, validating, and investigating cases, as well as tracing the movement of illicit funds across payment rails and freezing stolen funds before they move beyond reach.

3.1 Malaysia: Central Bank and FMI as Partners in National Fraud Response

Malaysia provides perhaps the most advanced and instructive case study of how national fraud response can be organised through a partnership between the central bank and the national payment infrastructure. Bank Negara Malaysia (BNM) has been the driving force behind the country's fraud response strategy, establishing the National Scam Response Centre (NSRC) in 2022 and housing it within the central bank's own operations. The NSRC brought together law enforcement, financial institutions, and regulators under BNM's coordination, laying the groundwork for a unified national response. This framework was significantly enhanced with the introduction of the National Fraud Portal (NFP) in August 2024 (Bank Negara Malaysia, 2024).

For the technical platform underpinning the NFP, BNM designated PayNet, Malaysia's national payments network and central financial market infrastructure,[1] as the operator. This pairing of central bank leadership with FMI execution was a deliberate design choice. As the operator of Malaysia's real-time payment rails (DuitNow), interbank clearing systems, and shared banking infrastructure, PayNet already maintains direct technical connections to all major financial institutions and has established governance frameworks for multi-stakeholder cooperation. BNM's regulatory authority and convening power, combined with PayNet's operational reach and technical connectivity, created a model in which the central bank sets the strategic direction and supervisory framework while the FMI provides the platform through which institutions collaborate in real time.

The results have been substantial. According to Malaysia's Deputy Minister of Finance, speaking in Parliament in October 2024, the NFP had reduced the time required to trace funds by 75 per cent, to 30 minutes, and increased the amount of funds frozen by 28 per cent since it began operating (Bernama, 2024). Case resolution times have been reduced dramatically: at the 2026 Global Fraud Summit, a Deputy Governor of Bank Negara Malaysia reported that end-to-end investigation times have been brought down to as little as ten minutes (Global Fraud Summit, 2026). This acceleration was enabled by capabilities including automated real-time tracking of fraudulent transactions and collaborative case management across more than 50 participating institutions (PayNet, n.d.), with over 500 case officers working from a single shared platform.

The broader lesson from Malaysia is institutional, not merely technological. The success of the NFP rests on the partnership model: a central bank providing strategic leadership, regulatory authority, and supervisory oversight, working in tandem with a trusted FMI that has existing connectivity to the financial ecosystem and access to transactional data, and serves as a neutral platform for multi-stakeholder coordination. This central bank–FMI partnership reduces the barriers to participation,

[1] PayNet (Payments Network Malaysia Sdn Bhd) is the national payments network and shared central infrastructure for Malaysia's financial markets. It operates under the oversight of Bank Negara Malaysia and serves as the operator of multiple payment systems including DuitNow, Malaysia's real-time payment platform.

ensures regulatory alignment, and creates the trust necessary for institutions to share sensitive fraud data. It is a model with clear relevance to the Arab region, where central banks similarly operate or oversee the national payment systems.

3.2 Other National Approaches

Indonesia offers a contrasting route. Its Anti-Scam Centre, operating since November 2024 under the Financial Services Authority (OJK), receives victims' reports and coordinates the blocking of accounts across banks, and OJK has announced that participation will be mandatory for all banks (Antara News, 2024; The Jakarta Post, 2025). Between November 2024 and October 2025, it received 299,237 reports, blocked 94,344 accounts, and recovered IDR 376.8 billion (Antara News, 2025). In parallel, Bank Indonesia, the central bank, is developing fraud prevention capabilities within its BI-FAST instant payment system, including mechanisms for sharing mule account data across participating institutions. Indonesia thus combines a supervisor-led response centre with fraud controls in the central bank's payment system, rather than the single central bank–FMI partnership of the Malaysian model.

Within the Arab region, important developments are underway, with central banks taking the lead in establishing national fraud coordination capabilities, a pattern consistent with their role as operators of the national payment systems. The approaches vary, reflecting different starting points and institutional contexts, but share a common direction. The Central Bank of the UAE has begun establishing the Central Bank Anti-Fraud Operations Center (CAFOC), conceived as "a central operational and intelligence hub" for real-time fraud monitoring, rapid incident response, and closer coordination with licensed financial institutions and other stakeholders. Its tracing tools, escalation procedures, and coordination across the sector are intended to underpin an intelligence-driven response to fraud and to consolidate fraud insights for supervisory and policy purposes (Central Bank of the United Arab Emirates, 2025, p. 90). Another central bank has convened a working group to develop a national fraud portal, recognising that centralised fraud response capabilities are becoming essential as its digital payments ecosystem grows rapidly. A third has established a formal consortium with its major commercial banks to serve as the institutional foundation for a national fraud coordination platform, and is developing fraud utility guidelines in parallel. Elsewhere in the region, a central bank has issued a request for information on advanced fraud detection technologies and is evaluating options for a national fraud detection pilot, building on its existing consumer complaint infrastructure.

These developments highlight the growing momentum across the region, though the pace of adoption varies. The experience of early movers internationally illustrates the measurable benefits of national fraud coordination. As instant payment volumes grow across Arab countries, jurisdictions that establish such capabilities will be better positioned to protect consumers, meet evolving FATF evaluation standards, and contribute to cross-border cooperation.

Table 1 compares Malaysia, Indonesia, and the United Arab Emirates on the four dimensions set out in Section 1.

Table 1: National cases compared

	Malaysia	Indonesia	United Arab Emirates
Governance and legal mandate	Bank Negara Malaysia leads; National Scam Response Centre within the central bank since 2022	Financial Services Authority (OJK) leads the Anti-Scam Centre; participation mandatory for all banks	Central Bank of the UAE; Anti-Fraud Operations Center (CAFOC) being established
Operating model and connection to payment rails	PayNet, operator of the DuitNow real-time payment rails, runs the National Fraud Portal (since 2024)	Anti-Scam Centre receives reports and coordinates account blocking; Bank Indonesia developing fraud prevention within BI-FAST	Central operational and intelligence hub with tracing tools and escalation procedures
Data-sharing arrangements	More than 50 participating institutions and over 500 case officers on one shared platform	Account reports shared across banks through the Anti-Scam Centre; mule account data sharing across BI-FAST participants in development	Coordination with licensed financial institutions; fraud insights consolidated for supervisory and policy purposes
Reported results	Tracing time cut by 75 per cent, to 30 minutes; funds frozen up 28 per cent	299,237 reports, 94,344 accounts blocked, and IDR 376.8 billion recovered (November 2024 to October 2025)	Not yet reported

Sources: Sections 3.1 and 3.2; Bernama (2024); PayNet (n.d.); Antara News (2024, 2025); Central Bank of the United Arab Emirates (2025).

3.3 Impact of National Anti-Scam Utilities

The impact of NASUs is multi-dimensional. They enable real-time tracking and freezing of fraudulent funds, compressing the response cycle from days to minutes. Case officers across participating institutions are alerted in parallel, ensuring that funds are earmarked simultaneously across banks and payment rails.

NASUs also introduce a collaborative utility in which financial institutions, supervisors, and law enforcement work from a single incident record, removing duplication and enabling system-wide case prioritisation. By pooling transaction networks across banks, NASUs enhance machine learning models through validated feedback loops, providing a holistic view of how funds propagate that outperforms institution-level models (Molloy et al., 2017). Central banks gain real-time insights into systemic fraud risks, enabling them to identify emerging typologies and calibrate regulatory measures accordingly.

More broadly, national fraud coordination capabilities are increasingly understood as a dimension of payment system sovereignty. The ability to trace and disrupt illicit financial flows across the domestic payment network, in real time and under the authority's own control, is a core function of sovereign financial infrastructure. Countries that lack this capability are dependent on individual institutions or external providers to safeguard the integrity of their payment systems, a dependency that carries both operational and strategic risks. Investing in national fraud coordination is therefore not only a response to rising fraud losses but an investment in financial stability, consumer protection, and the sovereign resilience of the financial system itself.

The evidence from these deployments is clear. A jurisdiction operating an instant payment system requires a coordinated national capability to detect, trace, freeze and recover funds, and to analyse the resulting data. That capability is a prerequisite for consumer protection and for the integrity of the financial system. Its institutional form is a national choice.

Despite their demonstrated impact, national solutions remain bounded by jurisdictional borders. Fraud schemes, particularly those involving transnational organised networks and digital assets, often span multiple countries. NASUs can close the gap within a domestic ecosystem, but they cannot independently address the complexity of cross-border fraud flows. Equally, cross-border fraud coordination cannot function without capable domestic counterparts: a regional alert or intelligence-sharing mechanism is only effective if there is a national system on the receiving end that can act on it in real time. This points to two complementary and sequential priorities: first, establishing national fraud coordination capabilities where they do not yet exist, and second, designing both existing and future NASUs with cross-border interoperability in mind from the outset.

4. The Cross-Border Challenge

NASUs serve as a vital line of defence within national borders, but lack mechanisms to trace funds or share information across jurisdictions. The same characteristics that make cross-border fast payment platforms effective also make them vulnerable to criminal exploitation. Lessons from Europe are instructive: following the introduction of SEPA and instant payments, cross-border transactions came to account for 71% of card fraud by value, 43% of credit transfer fraud, and 47% of direct debit fraud, while information-sharing processes between financial intelligence units remained slow, manual, and fragmented (EBA & ECB, 2024).

For the Arab region, the implications are direct. The GCC states have made significant progress in deepening regional integration, and all six GCC countries now operate domestic fast payment systems. Buna is establishing the foundation for cross-border instant payment connectivity across Arab countries. Buna already supports settlement in seven currencies, and its membership base spans over one hundred financial institutions across the GCC, Levant, and North Africa (Central Bank of the United Arab Emirates, 2022; Arab Monetary Fund, 2023). Recent agreements with Egypt's national instant payment operator and with Pakistan's Raast platform further extend Buna's reach (Emirates News Agency, 2023). These infrastructures are essential for economic development and regional integration. Yet, unless fraud resilience is considered alongside payment efficiency, the features that drive integration could also be exploited by those seeking to move illicit funds across borders.

4.1 FATF and MENAFATF Recommendations on Information Sharing

The effectiveness of cross-border fraud detection is constrained by the absence of harmonised, machine-readable standards for information exchange. FATF guidance urges jurisdictions to create legal frameworks and safe harbours enabling private sector information sharing (Financial Action Task Force, 2017a, 2017b, 2025), and the Egmont Group's Principles affirm that cross-border FIU collaboration is essential (Egmont Group, 2025). A significant recent development is the FATF's Roadmap 26-28 on Combatting Fraud, launched in July 2026, under which the FATF will work to enhance public-private, cross-border, and private-to-private information sharing, so that countries can keep pace with the speed at which illicit finance moves across institutions and borders (Financial Action Task Force, 2026). This creates a new imperative for jurisdictions to demonstrate operational effectiveness, including in cross-border cooperation.

In the Arab region, MENAFATF assesses its members against these standards through mutual evaluations of both technical compliance and effectiveness, and follows up on the deficiencies they

identify (MENAFATF, n.d.). The gap between instant payment settlement speed (seconds) and cross-border intelligence exchange (days or weeks) represents a structural vulnerability. National fraud-detection utilities have begun to bridge this gap domestically through public-private partnerships (Asian Development Bank, 2024), but once funds cross borders, differences in data protection laws, legal mandates, and interoperability standards constrain the ability to share actionable intelligence at a comparable speed.

4.2 The Cross-Border Limits of National Utilities

National-level responses, while essential, face inherent limitations when confronting transnational fraud. Freezing orders are bounded by jurisdictional borders and rarely recognised across countries in real time. Mule account detection ends at the border, as NASUs have no visibility into foreign transaction trails. Intelligence on fraud typologies and compromised devices remains fragmented across divergent privacy regimes and supervisory mandates. Case management processes are duplicative, with law enforcement in different countries often repeating investigative steps in isolation.

4.3 Cross-Border Intelligence Sharing in Practice

International collaboration has improved the detection, disruption and recovery of fraud. The examples below fall into two categories. The first covers the exchange of fraud intelligence between financial institutions and financial intelligence units. The second covers the coordination of law enforcement action and the recovery of assets. The two operate under different mandates, on different timescales, and under different legal authorities. Section 5 addresses the first category.

The Global Anti-Scam Alliance (GASA) has established the Global Signal Exchange, a shared repository of fraud indicators including phone numbers, URLs, and device identifiers associated with scam operations. The platform is offered free of charge to NASUs, providing a low-barrier mechanism for participating jurisdictions to both contribute to and benefit from collective intelligence. Integration of such signal-sharing capabilities with regional payment infrastructure could significantly enhance early detection of cross-border fraud.

Complementary initiatives show similar progress. SWIFT's 2025 pilot with 13 international banks used privacy-enhancing technologies to share suspicious-account indicators across borders, doubling detection rates in ten million test transactions without compromising confidentiality (SWIFT, 2025).

The Egmont Group has long fostered FIU-to-FIU cooperation through structured case sharing and legal principles. Its Best Egmont Cases (BECA) programme documents exemplary intelligence cases across jurisdictions, enabling member FIUs to learn from complex cross-border investigations (Egmont Group, 2024).

4.4 Law Enforcement Coordination

The mechanisms described below address the investigation of fraud and the recovery of assets rather than the exchange of intelligence. They operate on timescales measured in days and weeks rather than seconds, and under legal authorities held by police and judicial bodies rather than by financial institutions or payment system operators.

A leading example is FRONTIER+, the anti-scam operations platform launched in 2024 by law enforcement agencies across the Asia-Pacific region (Singapore Police Force, 2025). Through shared intelligence channels and joint enforcement protocols, FRONTIER+ has frozen over 32,000 bank accounts, recovered more than USD 20 million in scam proceeds, and enabled the arrest of 1,800 suspects in 9,200 cases within its first coordinated operation (Hong Kong Police Force, 2025; Singapore Police Force, 2025).

Interpol's I-GRIP (Global Rapid Intervention of Payments) mechanism and the recently introduced Silver Notice provide an enforcement-level complement to intelligence-sharing platforms. Through I-GRIP, Interpol coordinates with member countries to freeze fraudulent funds before they are dissipated. In one notable case, Singapore authorities used the mechanism to recover approximately USD 40 million from a single business email compromise fraud (Interpol, 2024). The Silver Notice, adopted in 2024, enables Interpol member countries to issue cross-border requests to trace and freeze criminal proceeds, creating a structured pathway for asset recovery that could be integrated with regional fraud coordination platforms.

Looking ahead, Interpol has announced plans to establish a Global Fraud Taskforce by 2029, focusing on three pillars: tactical enforcement (arrests and asset seizures), strategic disruption (sanctions, supply chain interference, and travel restrictions), and public-private partnerships to address industry enablers of fraud (UK Home Office, 2026). This initiative, if realised, would create a global enforcement layer that could complement regional coordination platforms.

The models in both categories demonstrate that secure, real-time cross-border collaboration is feasible and effective. They also indicate that governance matters as much as technology: results depend on trusted governance arrangements, clear legal frameworks, and operational neutrality.

5. Tools for Cross-Border Fraud Resilience

Cross-border fraud resilience requires a combination of technical, legal, and operational capabilities. This section outlines four building blocks that could be adopted incrementally and are mutually reinforcing: real-time track-and-trace (5.1), secure exchange of fraud intelligence (5.2), cross-border consumer case transparency and scam report intelligence (5.3), and privacy-preserving identity exchange (5.4). Several of these align with capabilities already envisaged in the AMF's Cyber Resilience Oversight Guidelines (AMF, 2019) and the Arab Region Fintech Guide (AMF, 2021). The specific combination and sequencing would depend on the priorities and readiness of participating jurisdictions. The tools described below address the intelligence layer set out in Section 4.3. They complement the law enforcement mechanisms set out in Section 4.4, which operate on different timescales and under different legal authorities.

5.1 Cross-Border Track and Trace

The first priority is the ability to trace and freeze funds across jurisdictions in real time. In a domestic NASU, track-and-trace functionality allows investigators to reconstruct the path of fraudulent transfers through multiple accounts and payment rails, flagging mule accounts and earmarking balances for recovery. Extending this capability across borders is important because of the asymmetry

between the speed of modern payment systems (which clear in seconds) and the slowness of current cross-border cooperation (which often takes days).

A key enabler is the transmission of standard transaction and trail identifiers across national systems. The use of unique end-to-end transaction references (UETRs), already embedded in ISO 20022 standards (International Organization for Standardization, n.d.) and in SWIFT's global payments innovation (GPI) (SWIFT, n.d.), can serve as anchors that link the domestic legs of a cross-border payment. As underscored by the BIS CPMI (2023), the use of unique identifiers and structured data is a prerequisite for achieving true interoperability across payment systems.

Crucially, effective cross-border track-and-trace does not require pooling all data in a central repository, an approach that would raise significant sovereignty and privacy concerns. Instead, a federated model could be adopted, whereby each jurisdiction retains control of its own payment data and responds to authorised queries through secure, standardised interfaces. This federated design preserves each jurisdiction's sovereign control over its own data while enabling collective capability that no single jurisdiction could achieve alone. It ensures that participation in cross-border fraud coordination strengthens, rather than diminishes, national oversight.

5.2 Cross-Border Secure Exchange of Fraud Intelligence

Once jurisdictions can trace funds in real time within their own systems, a further step is the secure exchange of intelligence. Conventional mechanisms, relying on manual FIU-to-FIU requests, are incompatible with the speed of instant payments. Privacy-enhancing technologies (PETs), including secure hashing and multiparty computation (MPC), allow institutions to match fraud-related data without disclosing underlying personally identifiable information. Intelligence outputs such as pseudonymised risk scores could be transmitted back into domestic systems, creating a feedback loop that enhances collective detection capability while preserving each jurisdiction's sovereign control over its data, a principle already established in the federated architecture described in 5.1

The potential of this approach has been demonstrated in practice. In 2025, SWIFT published the results of experiments conducted with 13 global financial institutions in which PETs were used to enable secure cross-border sharing of fraud insights. In one use case, PETs enabled participants to verify intelligence on suspicious accounts in real time; in another, they were used to identify anomalous transaction patterns. Across ten million test transactions, the collaborative model was twice as effective at identifying known fraudulent transactions compared to models trained on a single institution's dataset (SWIFT, 2025). Project Aurora, a proof-of-concept led by the Bank for International Settlements in collaboration with multiple central banks, demonstrated a comparable approach for cross-border money laundering detection, validating the use of privacy-enhancing technologies to identify criminal patterns spanning multiple jurisdictions without centralising sensitive data (BIS Innovation Hub, 2023).

Looking further ahead, federated learning (a technique in which an AI model trains locally on each institution's data without the underlying information leaving that institution) offers potential for more sophisticated cross-border pattern detection. However, standard implementations can suffer from model misconvergence when institutions' data differ significantly in fraud typologies, transaction volumes, or labelling conventions. More robust algorithmic approaches exist to mitigate this, but they presuppose a baseline of harmonised data standards and shared fraud classification conventions

across participating jurisdictions. This makes the standardisation work described in 5.1 a prerequisite for any future deployment of this kind, and underscores a broader point: the value of cross-border intelligence sharing grows in proportion to the consistency and quality of the data that participating jurisdictions contribute.

Sustainable cooperation across all these approaches would also require standardised message formats, secure APIs, and governance protocols to ensure shared intelligence remains interoperable, auditable, and actionable, aligned with Egmont and FATF guidance.

5.3 Cross-Border Consumer Case Transparency and Scam Report Intelligence

A dimension of cross-border fraud resilience that is often overlooked is the consumer-facing layer: the ability to keep victims informed about the status of their case as it progresses across jurisdictions, and to leverage the rich data contained in consumer scam reports for cross-border detection and prevention. These two functions are distinct but complementary, and both depend on the cross-border connectivity established in the preceding sections.

When a fraud case crosses borders, the victim typically loses all visibility into what is happening. Domestic authorities may refer the case to a counterpart jurisdiction, but there is rarely a mechanism to relay updates back to the consumer. This erodes trust in the system and discourages future reporting. A regional framework could address this by enabling standardised case-status notifications that flow back through the originating NASU to the consumer, even when the investigation has moved to another jurisdiction. Such a mechanism would not require sharing case-sensitive details, only structured status updates (such as “case received,” “funds located,” or “recovery in progress”) that keep the victim informed without compromising operational security.

Equally valuable is the intelligence embedded in consumer scam reports themselves. When victims report fraud, they provide detailed narratives: how they were contacted, what platform was used, what instructions they received, what documents or links were shared, and how the payment was initiated. This unstructured data, when aggregated across jurisdictions, contains patterns that are invisible at the national level. For example, a social engineering script that appears in reports across three Arab countries may indicate a single organised campaign, while clusters of similar contact methods or payment routing patterns can reveal emerging typologies before they are reflected in transaction monitoring systems.

Recent advances in natural language processing and automated classification make it feasible to operationalise this intelligence at scale. Analytical capabilities that extract, classify, and cross-reference information from unstructured scam reports could process incoming consumer reports, identify structured indicators (contact channels, scam narratives, payment methods, device information), and match them against reports from other jurisdictions in near real time, all while preserving the privacy of individual victims through appropriate anonymisation and aggregation techniques. A regional coordination layer could enable participating jurisdictions to benefit from collective pattern recognition without centralising sensitive personal data.

5.4 Privacy-Preserving Identity Exchange

A further and more sensitive layer concerns the exchange of verified identity information linked to mule accounts, compromised credentials, or fraudulent devices. While transaction trails and risk

scores can often be shared in pseudonymised form, there are circumstances in which law enforcement and financial institutions require access to identity-level data to conclude an investigation or initiate asset recovery. Yet identity data represents the most regulated and privacy-sensitive category of information and its exchange across borders requires careful design.

Multi-party computation (MPC) protocols (which differ from their application in 5.2 in that they operate on identity-level rather than transaction-level data) could allow two or more parties to jointly compute whether a suspect identity matches across jurisdictions without revealing the underlying personal data to either party. Cryptographic obfuscation techniques, such as proxy identifiers or salted hashes, offer complementary protection. Zero-knowledge proofs (ZKPs) could further strengthen privacy by allowing one jurisdiction to demonstrate that a specific condition is true without revealing the dataset itself.

Robust access control frameworks would be essential to govern when and how identity data can be shared. Importantly, disclosure protocols would need to be harmonised with privacy and data protection laws across the Arab region, which encompasses diverse legal traditions including civil law, common law, and Sharia-influenced commercial law, to avoid legal conflicts that could undermine cooperation.

6. Exploring Buna's Potential Role in Regional Fraud Resilience

6.1 Buna's Legal Foundation and Objectives

Buna, formally the Arab Regional Payments Clearing and Settlement Organization (ARPCSO), was established by the AMF as a specialised international organisation with legal personality, immunities, and privileges. This status means that Buna operates independently of any single national jurisdiction, and that data processed through its systems is protected from unilateral access, seizure, or interference by any individual state. Its core objectives include enabling safe, cost-effective cross-border settlement in Arab and international currencies, promoting the use of Arab currencies in regional trade, and supporting financial integration, aligned with the AMF's broader mandate.

Buna has an independent Board of Directors and is subject to the oversight of central banks whose currency is an accepted settlement currency by the system. Its rules and procedures define roles, responsibilities, liabilities, and operational standards for all participants, creating a shared legal and operational baseline developed through extensive consultation with central banks and financial institutions across the region.

6.2 Buna's Existing Capabilities

Buna has been operational since 2021. It currently serves over one hundred financial institutions, supports settlement in seven currencies (AED, SAR, JOD, EGP, USD, EUR and CNY), and provides both real-time gross settlement (RTGS) and instant payment services (IPS). Its participants include financial institutions in the Arab region and beyond.

Buna is connected to China's Cross-Border Interbank Payment System (CIPS) through Bank of China, and its interlink with Pakistan's Raast instant payment system is expected to go live in 2027. Mastercard joined as a participant in 2024, and Visa as a participant in 2026. A joint BIS, IMF, and

World Bank analysis identified Buna as one of four regional multilateral platforms for cross-border payments, alongside PAPSS, TIPS, and LankaPay (BIS CPMI, IMF & World Bank, 2023).

Buna currently applies a rule-based framework of scenarios and typologies to screen transactions for potential fraud, money laundering, and terrorism financing indicators. Although focused on compliance with AML/CFT standards, this capability provides an operational baseline for transaction-level screening in a cross-border context. The question explored in this paper is whether and how this baseline could be extended to address the evolving fraud landscape described in earlier sections.

As Buna extends its connectivity through interlinking agreements with national instant payment systems, the question of fraud monitoring and money tracing has increasingly arisen in discussions with partner jurisdictions. The tools and approaches discussed in Section 5 describe how the region could progressively build upon Buna's existing screening capabilities.

6.3 The FMI Model: From PayNet to Buna

The Malaysian experience, discussed in Section 3, offers a structural parallel that is relevant to the Arab region. In Malaysia, Bank Negara Malaysia provided the strategic leadership and regulatory authority, while PayNet, as the trusted national FMI with existing connections to all major banks, served as the platform operator for the National Fraud Portal. The success of this central bank–FMI partnership was driven by the combination of regulatory convening power and operational connectivity.

At the regional level, Arab central banks are establishing national fraud coordination capabilities and, in many cases, operate the domestic payment systems. Buna, as an international organisation owned by the AMF, has existing connectivity to over one hundred financial institutions across the Arab region, and its rules and procedures define roles, responsibilities, and liability frameworks for participating entities. These characteristics are relevant to the question of how cross-border fraud coordination might be structured.

This does not mean that the Malaysian model should be replicated directly, as the cross-border context introduces additional complexity around sovereignty, legal harmonisation, and varying levels of institutional readiness. However, the underlying principle is worth examining: a partnership between central banks and a trusted regional FMI, mirroring the BNM–PayNet model at a cross-border scale, could reduce the barriers to participation and ensure that fraud coordination operates within an established governance and oversight framework.

6.4 National Anti-Scam Utility Integration with Buna's Settlement Layer

As Arab countries establish National Fraud Portals (NFPs) and other National Anti-Scam Utilities, a natural question arises: how could these national capabilities connect to Buna's cross-border settlement infrastructure to create a more integrated fraud response? One possibility worth exploring is the concept of pre-settlement fraud screening, whereby Buna's settlement logic could incorporate signals from national fraud coordination systems before a cross-border payment is finalised.

In its simplest form, this could operate as a 'red-light' alert mechanism. When a cross-border payment instruction is submitted through Buna, the platform could query the relevant jurisdiction's NASU for active fraud flags on the beneficiary account, transaction pattern, or related identifiers. A positive

signal, such as a suspected mule account or active investigation, would pause settlement and trigger a structured review workflow involving the relevant institutions and national authorities, rather than constituting a unilateral block, unless a mandatory threshold of the kind discussed below applies.

The technical prerequisites align with the building blocks in Section 5: standardised transaction identifiers (UETRs) for matching, API-based query interfaces for real-time lookups without bulk data transfers, and the federated architecture ensuring each jurisdiction retains sovereign control over its fraud data. This model would become more effective as more jurisdictions bring their NASUs online, creating a network effect. For jurisdictions in the early stages, designing their national systems with future Buna connectivity in mind, through common data standards and API specifications, would reduce integration costs when the time comes.

Several questions of operating model would need to be settled before such an arrangement could be built. They are set out here for discussion. The first concerns how participants use a signal generated by Buna. Under an advisory model, the signal is one input to each participant's own fraud decisioning, and the participant decides whether to act on it. Under an authoritative model, the signal is the primary risk score for the transactions Buna processes, and participants align their handling to it. Buna could also set mandatory thresholds above which a transaction is paused or rejected, whatever an individual participant would otherwise do. A combination of these approaches is possible, with participant discretion in the ordinary range and mandatory controls at the extreme, and the boundary between them would need to be defined.

Each model carries consequences for Buna's rules and procedures. What legal basis supports pausing or rejecting a payment instruction on a fraud signal, as distinct from the AML and CFT grounds on which screening operates today, and how does that basis interact with settlement finality? How is liability allocated when funds are released despite an accurate signal, and when a legitimate payment is delayed or rejected on an inaccurate one? Who sets and revises the thresholds, on what evidence, and under whose oversight? Who may release a paused transaction, within what time, and on what record? How would a jurisdiction that has not yet established a national utility take part, and would a regionally derived signal be available to its institutions in the meantime? These are questions for the Board of Buna, its participating central banks, and the relevant national authorities. The authors take no position on them in this paper.

Pre-settlement screening would not eliminate the need for post-settlement cooperation, but it could significantly reduce the volume of fraudulent transfers that succeed in the first instance, shortening the window between fraud execution and response from days to seconds.

6.5 The Potential Value of a Regional Coordination Layer

In a traditional cross-border fraud detection arrangement, each NASU would need to establish bilateral connections with every other participating NASU. In a region of 22 Arab countries, this would require over 230 bilateral arrangements. Each connection demands its own technical integration, operational monitoring, legal agreements, and ongoing maintenance.

Under a hub-and-spoke model, each NASU would connect once to a regional coordinator and gain access to the entire network. Such an approach could address these challenges by reducing integration burdens, lowering costs, and accelerating implementation. As countries establish their national fraud coordination capabilities, designing them with future cross-border connectivity in mind would allow

them to participate in a regional network when the time is right. Buna's existing architecture and connections with central banks and financial institutions are relevant to this model.

6.6 Sovereignty, Security, and Strategic Resilience

A significant concern in cross-border fraud detection is ensuring that sensitive financial and operational data remains secure while respecting the sovereignty of all participating jurisdictions. In an environment where payment infrastructure is increasingly recognised as critical national infrastructure, and where financial data can be subject to extraterritorial legal claims, geopolitical pressures, or unilateral access by foreign authorities, the institutional framework within which fraud intelligence is shared matters as much as the technical capabilities deployed.

Buna's status as an international organisation established by the AMF means that data processed through its systems operates within a multilateral governance framework, with oversight from participating central banks. For Arab countries seeking to strengthen their fraud coordination capabilities, this offers the advantage of building on an institution that is already governed by and accountable to the region's own financial authorities, ensuring that any future fraud intelligence functions would develop within an existing framework of regional cooperation and shared oversight.

Sovereign control over financial intelligence, including the ability to detect and trace illicit flows within and across national payment systems, is a component of broader financial system sovereignty. A regional approach anchored in an institution governed by the region's own central banks would keep this intelligence function under collective regional control, rather than depending on external platforms whose governance structures may not align with the region's interests.

6.7 Interoperability with Other Regional Hubs

While the primary objective would be to strengthen fraud resilience within the Arab region, the design of any regional framework should anticipate eventual interoperability with similar initiatives emerging globally. Several complementary efforts are already underway: the BIS Nexus project in Southeast Asia, the Pan-African Payment and Settlement System (PAPSS), the CARICOM Payments and Settlement System (CAPSS), and TIPS in the euro area and Western Balkans.

Buna's interlinking agreements with payment systems in other regions mean that it already operates across several geographies. Any fraud response layer built within this network would benefit from being interoperable by design, through standardised data formats, privacy-preserving protocols, and mutual recognition mechanisms, enabling the Arab region to contribute to a globally coordinated response to financial crime.

7. Conclusion

The rapid growth of instant and cross-border payments has made fraud not only faster but also harder to detect and contain, especially as criminal actors gain the ability to move funds across jurisdictions in seconds. The rise of National Anti-Scam Utilities marks a significant advance in national-level resilience, and establishing these domestic capabilities is the essential foundation: cross-border fraud coordination can only be as effective as the national systems it connects. As more jurisdictions build these capabilities, the opportunity to link them through interoperable, secure, and privacy-preserving mechanisms becomes both more feasible and more valuable.

International experience, notably the PayNet model in Malaysia and SWIFT's privacy-preserving pilots, demonstrates that trusted financial market infrastructures can serve as effective coordination platforms for fraud response. Law enforcement initiatives such as the FRONTIER+ platform in Asia-Pacific show that cross-border collaboration is both technically feasible and operationally impactful.

Arab countries have a track record of building shared financial infrastructure. Extending this to encompass fraud resilience would protect consumers, strengthen financial stability, and enable the region to contribute to global efforts against cross-border financial crime. Buna's status as an international organisation, sponsored and overseen by central banks, and its operational connectivity across the Arab region are characteristics that are relevant to the question of how cross-border fraud coordination might be organised. The options explored in this paper, ranging from standardised identifiers and federated track-and-trace to privacy-preserving intelligence sharing and advanced identity exchange, represent building blocks that could be adopted at a pace determined by the region's stakeholders.

For jurisdictions that have not yet established national anti-fraud coordination capabilities, the evidence presented in this paper suggests that the capability a NASU provides is a prerequisite for any country operating an instant payment system. Its institutional form is a matter for each jurisdiction to determine. The experience of Malaysia, the most fully documented case, shows that coordinated national fraud response can substantially improve detection rates, fund recovery, and consumer protection. Such a capability is also the foundation on which successful cross-border fraud response is built.

Bibliography

Al Arabiya English. (2022, November 9). Cybercriminals impersonate Saudi recruitment firm to infiltrate bank accounts.

Amerhauser, K., & Goodwin, A. (2026, March). A world of deceit: Mapping the landscape of the global scam centre phenomenon. Global Initiative Against Transnational Organized Crime.

Antara News. (2024, August 2). OJK to necessitate all banks to join Anti-Scam Center team.

Antara News. (2025, October 21). OJK urges scam victims to report within 10 minutes to recover funds.

Arab Monetary Fund. (2019). Cyber Resilience Oversight Guidelines for the Arab Countries, Concerning Financial Market Infrastructures. Abu Dhabi: AMF.

Arab Monetary Fund. (2020). Fintech Strategy Guidelines for the Arab Region (Publication No. 140). Abu Dhabi: AMF.

Arab Monetary Fund. (2021). The Arab Region Fintech Guide, Second Edition (Publication No. 166). Abu Dhabi: AMF.

Arab Monetary Fund. (2023, November 7). Banks go live on Buna's Payment versus Payment (PvP) service, providing safer settlement.

Asian Development Bank. (2024). Financial crimes compliance: The power of partnerships. Manila: ADB.

Bank Negara Malaysia. (2024, August 20). Launch of the National Fraud Portal (NFP) to strengthen Malaysia's response to scams and fraud.

Bernama. (2024, October 22). National Fraud Portal cuts fund-tracing time to 30 minutes, boosts frozen funds.

BIS, Committee on Payments and Market Infrastructures. (2023, October). Harmonised ISO 20022 data requirements for enhancing cross-border payments. Basel: BIS.

BIS, Committee on Payments and Market Infrastructures, & Arab Monetary Fund. (2024). Monitoring cross-border payment developments: A regional analysis of AMF member countries (CPMI Brief No. 2). Basel: BIS.

BIS, Committee on Payments and Market Infrastructures, IMF, & World Bank. (2023, January). Exploring multilateral platforms for cross-border payments (CPMI Papers No. 213). Basel: BIS.

BIS Innovation Hub. (2023, May). Project Aurora: The power of data, technology and collaboration to combat money laundering across institutions and borders. Basel: BIS.

Central Bank of Egypt. (2024, September 8). The Central Bank of Egypt hosts the first edition of "Egypt Fraud Combating Forum".

Central Bank of the United Arab Emirates. (2022, July 28). Buna: Arab Regional Payment System.

Central Bank of the United Arab Emirates. (2025). Central Bank Annual Report 2025. Abu Dhabi: CBUAE.

EBA & ECB. (2024). Report on payment fraud. Frankfurt: European Banking Authority / European Central Bank.

Egmont Group. (2024). BECA III report 2021–2023: Best Egmont case award compilation.

Egmont Group. (2025). Principles for information exchange between financial intelligence units (Revised July 2025).

El Murr, A., Duvnjak, S., & Delechat, C. (2023). The role of the private sector in detecting and preventing illicit financial flows. In Enhancing the Effectiveness of AML/CFT Policies (pp. 19–36). Washington, DC: IMF.

Emirates News Agency. (2023, November 3). AMF, SBP sign MoU to facilitate cross-border remittances between Arab region and Pakistan.

Emirates News Agency. (2024, November 28). 2024 State of Scams in UAE survey reveals 65% scam awareness.

Financial Action Task Force. (2017a, November). Private sector information sharing.

Financial Action Task Force. (2017b, November). Consolidated FATF standards on information sharing.

Financial Action Task Force. (2025, June). International standards on combating money laundering and the financing of terrorism & proliferation.

Financial Action Task Force. (2026, July 1). FATF Roadmap 26-28 on Combatting Fraud. Paris: FATF.

Global Anti-Scam Alliance. (2024). Global State of Scams Report 2024. The Hague: GASA.

Global Fraud Summit. (2026, March). Plenary session statements and panel proceedings, Vienna.

Gulf News. (2024). Kuwait cryptocurrency scam: 40 million dinars lost in 'Bitcoin Kuwait' fraud.

Hong Kong Police Force. (2025, June 3). Seven countries and regions collaborate in cross-border anti-fraud initiative: "FRONTIER+" achieves significant results in first joint operation. Anti-Deception Coordination Centre.

International Organization for Standardization. (n.d.). ISO 20022: Universal financial industry message scheme.

Interpol. (2024, August 6). Police recover over USD 40 million from international email scam. Lyon: Interpol.

Interpol. (2025, July). Globalization of scam centres: New information on expansion beyond Southeast Asia. Lyon: Interpol.

LexisNexis Risk Solutions. (2024, April 17). Every dirham lost to fraud in UAE costs firms AED 4.19 according to LexisNexis True Cost of Fraud Study [Press release].

MENAFATF. (n.d.). Mutual evaluations and follow-up: Overview.

Molloy, I. et al. (2017). Graph analytics for real-time scoring of cross-channel transactional fraud. In Financial Cryptography and Data Security. FC 2016. LNCS, vol 9603. Springer.

Nasdaq Verafin. (2024). 2024 Global Financial Crime Report: Insights at the intersection of financial crime data and real survivor stories.

PayNet. (n.d.). National Fraud Portal.

Pindrop. (2025, June 12). 2025 Voice Intelligence & Security Report.

Saudi Central Bank. (2022, October). Counter-Fraud Framework (Version 1.0). Riyadh: SAMA.

Singapore Police Force. (2025, August 18). Operation FRONTIER: A united front against transnational scams.

SWIFT. (2025, September 15). SWIFT AI innovation creates blueprint for banks to stop fraud faster through cross-border collaboration.

SWIFT. (n.d.). SWIFT gpi: The standard in global payments innovation.

The Jakarta Post. (2025, February 11). OJK launches Indonesia Anti-Scam Centre to combat fraud.

TRM Labs. (2025, May 7). AI-enabled fraud: How scammers are exploiting generative AI.

UAE Financial Intelligence Unit. (2024, November 29). Organised financial fraud.

UK Home Office. (2023, May). Fraud Strategy: Stopping Scams and Protecting the Public. London: HM Government.

UK Home Office. (2026, March). Fraud Strategy 2026 to 2029: Disrupting crime, supporting economic resilience and delivering justice. London: HM Government.

UNODC. (2025, April). Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia. Bangkok: UNODC Regional Office for Southeast Asia and the Pacific.

Vogel, B. (2022). Potentials and limits of public-private partnerships against money laundering and terrorism financing. eucrim, (01), 52–60.