

Cyber-Prompted Frauds and AML/CFT Compliance

Emerging Challenges for
Pakistan's Financial Sector

By: Owais Ahmed Qureshi

Pakistan's financial sector has recently crossed a structural threshold. Digital channels now carry 92% of retail payment volume, up from 78% just three years ago, and the country's SBP backed instant-payment rail, RAAST, has helped push annual digital retail transactions from roughly 2.2 billion in 2021 to an estimated 8 billion in 2025. While, this shift has been good for financial inclusion, tax documentation, and investor confidence, it has been equally good for the fraudsters, as well. The National Cyber Crime Investigation Agency (NCCIA) and its predecessor, the FIA Cybercrime Wing, together received over 639,000 complaints between 2020 and 2025, with banking and digital fraud surging an estimated 62% in 2025 alone, against a backdrop of an overall 35% rise in cybercrimes.

Cyber fraud is not limited only to posing consumer-protection and balance-sheet related problems; it is increasingly recognized by the Financial Action Task Force (FATF) as a precursor to money-laundering and, in a growing number of documented typologies, a terrorist-financing risk. FATF's 2025 document/ publication, *Comprehensive Update on Terrorist Financing Risks*, found that terrorist actors are shifting toward decentralized, self-financed models that rely on low-value, high-frequency, technology-enabled funding streams the exact profile of proceeds generated by digital scams. For a country with Pakistan's terrorism and complexed terrorism-financing history, a near-zero cybercrime conviction rate (0.038% across 523,749 NCCIA complaints between 2023 and 2026), and an under-regulated virtual-asset sector only now being brought under a licensing regime, this is not a hypothetical concern. It is, as the subtitle of this piece suggests, a haunting threat that digital financial institutions can no longer treat as someone else's problem.

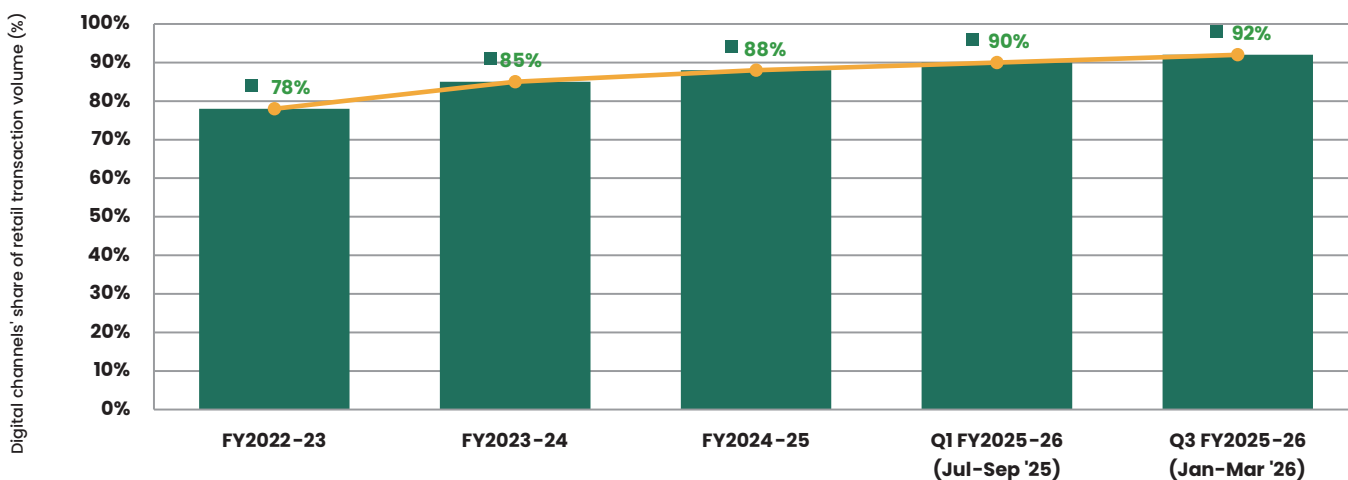
Pakistan's Digital Pivot: From a Cash Economy to a Cash-Light, Higher-Risk Economy

Pakistan has long been recognized as one of the world's largest cash-based economies, where physical currency dominated almost every layer of economic activity from household spending and wage payments to large commercial transactions. That dependence created a deeply undocumented economy: financial activity that left no audit trail, complicated tax collection, limited access to formal credit, and gave money launderers, tax evaders, and terror financiers room to operate largely undetected. It also excluded millions of

Pakistanis, particularly women, rural households, and small businesses, from formal financial services.

Over the past five years, that picture has changed faster than at any point in the country's financial history. The State Bank of Pakistan's (SBP) Electronic Money Institution (EMI) licensing framework along with newly awarded licenses for fully Digital Banks (NEO Banks) after a comprehensive digital framework and the RAAST instant-payment system have given Pakistan the regulatory and technological scaffolding for a digital-first financial ecosystem. The shift is no longer aspirational; it is measurable, quarter by quarter, in SBP's own payment-systems data.

Pakistan's Cash-to-Digital Transition Digital Share of Retail Payment Volume, FY2023 – Q3 FY2026



Source: SBP Annual & Quarterly Payment Systems Reviews (FY2023-Q3 FY2026); Raast launched Jan 2021.
Note: Comparable digital-share % is not published for FY2021-22; cash still dominates by transaction VALUE (~70%+ of value moves OTC/cash).

Figure 1: Pakistan's Cash-to-Digital Transition, FY2023–Q3 FY2026

Digital channels carried 78% of retail transaction volume in FY2022-23, rising to 85% in FY2023-24, 88% in FY2024-25, and 92% by the third quarter of FY2025-26 (Jan-Mar 2026), a trajectory reinforced by the RAAST Person-to-Merchant (P2M) rollout, the SBP Regulatory Sandbox, and the August 2025 go-live of PRISM+, Pakistan's modernized RTGS and central securities depository infrastructure. Annual retail transaction volume crossed 9.1 billion by FY2024-25. Every one of those milestones is, in compliance terms, a double-edged sword: each new digital rail is also a new attack surface. Remote onboarding, instant payment finality, and interconnected wallets have widened the field for phishing, social engineering, account takeover, identity theft, SIM-swap fraud, mule accounts, and AI-enabled scams risks which we will discuss further ahead.

Creating a Documented Economy

The shift from cash to digital is more than a technology upgrade; it is the foundation of a documented economy. Every digital transaction leaves an electronic record payer, recipient, amount, time, and purpose that did not exist in a cash transaction. For government, this means better visibility into economic activity and stronger tax collection. For AML/CFT purposes specifically, it means banks, EMIs, and regulators can deploy AI- and machine-learning-based transaction monitoring to flag unusual patterns and file timely Suspicious Transaction Reports (STRs) capabilities that simply do not exist over a cash counter. Every transaction that moves from cash to a regulated digital rail is, in effect, a transaction added to Pakistan's financial-crime visibility, not removed from it. The flip side, addressed later in this article, is that visibility is only useful if it is matched by investigative and prosecutorial capacity; a gap that still needs to be narrowed down in Pakistan.

“Every transaction that moves from cash to a regulated digital rail is, in effect, a transaction added to Pakistan's financial-crime visibility, not removed from it. The flip side, is that visibility is only useful if it is matched by investigative and prosecutorial capacity; a gap that still needs to be narrowed down in Pakistan.”

Pakistan's Population: A Strategic Asset and a National Exposure

With more than 240 million people nearly two-thirds under the age of 30 Pakistan's population could be one of its greatest digital-economy assets. Every new digital-wallet user adds value to the payment's ecosystem; every new EMI customer extends financial inclusion to someone previously locked out of formal finance. That scale seems to attract real investor interest in Pakistan's fintech sector and may emerge

into the rapid growth of EMIs, digital wallets, digital accounts, payment gateways, and merchant-acquiring platforms.

But scale cuts both ways. Millions of first-time digital users are entering the financial system every year with limited digital literacy, and Visa's 2024 consumer research found that approximately 55% of surveyed Pakistani consumers had been the target of a scam attempt, a figure that illustrates just how exposed a digitally inexperienced, digitally on-boarded population has become. Fraudsters exploit this gap through phishing, smishing (a form of cyberattack where scammers use deceptive text messages to trick you into clicking malicious links, revealing sensitive information, or sending money), vishing ('voice phishing') is a cybercrime where scammers use phone calls or voice messages to impersonate trusted organizations or individuals, manipulating victims into revealing sensitive personal or financial information), fake investment schemes, and increasingly AI-generated content that imitates banks, regulators, and trusted brands. Organized criminal networks recruit students, unemployed youth, and financially vulnerable people as money mules through fake job advertisements circulated on social media the same demographic and recruitment channel that extremist groups have historically used.

Global Milestones in Digital Payments: Lessons for Pakistan

Pakistan's digital transformation is not happening in isolation. India's Unified Payments Interface (UPI) has become a global benchmark for instant account-to-account payments; China's Alipay and WeChat Pay embedded digital payments into daily life; Brazil's Pix, Singapore's PayNow, the UK's Faster Payments Service, and Kenya's M-Pesa each demonstrate how digital infrastructure expands financial inclusion and reduces cash dependence. Open Banking, Central Bank Digital Currencies (CBDCs), and the global migration to the ISO 20022 messaging standard are the next layer of this evolution, promising richer transaction data and stronger AML/CFT screening for cross-border flows, a particularly relevant development for Pakistan as one of the world's largest remittance-receiving countries.



These international experiences carry a consistent lesson: sustainable digital-payment growth depends on more than technology. It depends on interoperability, merchant acceptance, consumer trust, and critically for this article's argument, a regulatory architecture that keeps pace with the speed of innovation. Pakistan has built much of the infrastructure (RAAST, the EMI framework, NADRA's digital-identity system). The open question, examined in the sections that follow, is whether it's supervisory and law-enforcement capacity has kept pace with the same speed.

When Innovation Attracts Crime: The Boom in Cyber-Enabled Fraud

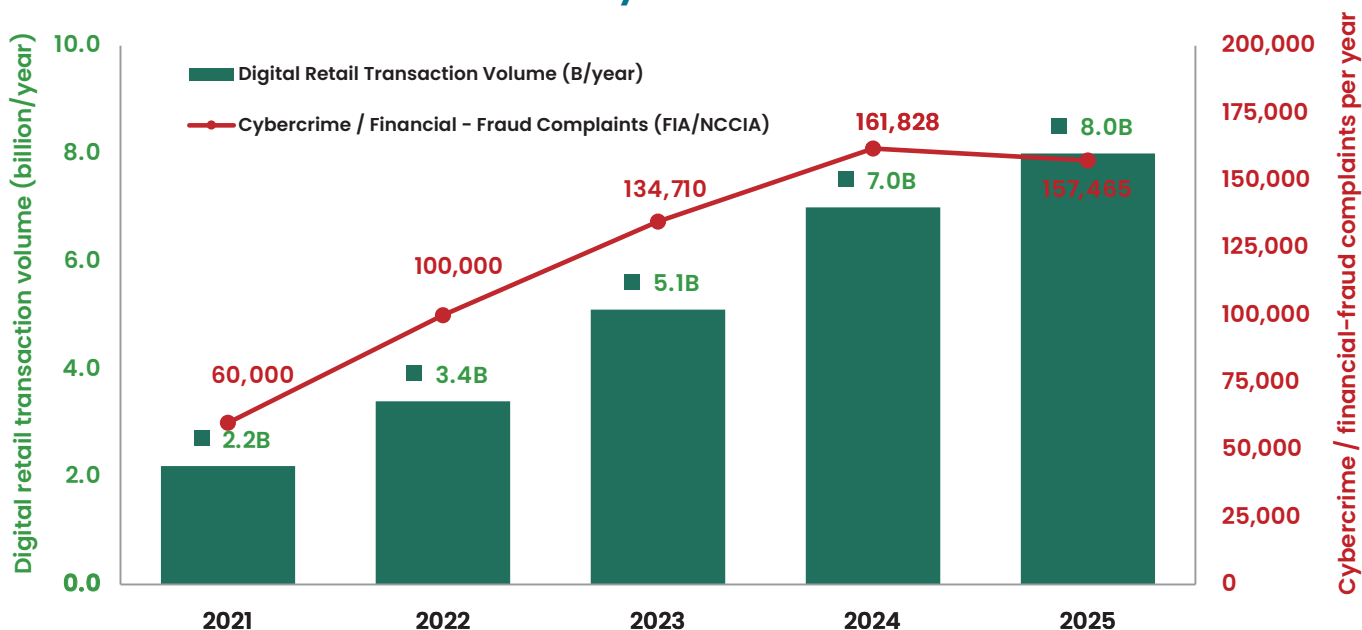
Financial crime has evolved in lockstep with digitalization. Today's criminals operate remotely through phishing, smishing, vishing, malware, QR-code manipulation, account takeover, identity theft, SIM-swap fraud, synthetic identities, investment and romance scams (when a fraudster creates a fake online identity to

build trust and affection with a victim, ultimately manipulating them into sending money or sensitive personal information), and Business Email Compromise. Generative AI has intensified the threat on both sides: criminals now produce convincing deep fake videos, cloned banking websites, and synthetic voice calls, while institutions deploy AI-driven transaction monitoring and behavioral analytics in response; an "AI-versus-AI" contest that the FATF itself has flagged as a defining feature of modern financial crime.

The scale of this is not a Pakistan-specific anomaly, it is a global pattern that Pakistan happens to be experiencing acutely. FATF's dedicated paper, *Cyber-Enabled Fraud Digitalization and Money Laundering, Terrorist Financing and Proliferation Financing Risks*, found that 156 jurisdictions 90% of those it assessed now identify fraud as a major money-laundering risk; that fraud accounts for more than 40% of all recorded crime in the United Kingdom; and that cyber-enabled scam cases in Singapore rose 61% in just two years.

Digitalization vs Fraud: Pakistan, 2021–2025

Growth in Digital Transactions Has Outpaced Pakistan's Capacity to Contain Cyber-Enabled Fraud



Sources: SBP Annual/Quarterly Payment Systems Reviews; FIA Annual Administration Reports (2021–22); NCCIA complaint data (2023–25). Digital volume figures are approximate annualised totals derived from SBP quarterly reviews. 2025 fraud dip reflects reporting/registration backlog, not reduced incidence – NCCIA officials cite a 35% surge in cybercrime and SBP reports a 62% rise in banking fraud in 2025.

Figure 2: Digitalization vs. Fraud – Pakistan, 2021–2025

“

Pakistan's fraud problem is not occurring despite digitalization, or merely alongside it; it is being generated by the same growth that is documenting the economy.”



In Pakistan, reported cybercrime and financial-fraud complaints rose from an estimated 60,000 in 2021 to 134,710 in 2023 (the year the NCCIA, National Cyber Crime Investigation Agency was established), 161,828 in 2024, and 157,465 in 2025 tracking almost exactly the same curve as the digital transaction volumes shown in Figure 1. This is the core observed link this article wants to draw out: Pakistan's fraud problem is not occurring despite digitalization, or merely alongside it; it is being generated by the same growth that is documenting the economy. Every successful fraud also produces a pool of illicit, low-trace proceeds that has to go somewhere.

Digital Scams Lead to Terror Financing: A Haunting Threat for Digital Financial Institutions

Terrorism doesn't need millions, it needs stealthy, frequent micro-payments that can support localized insurgencies or radicalization cells, and that is precisely the profile of proceeds a digital scam generates.

For most of its history, cyber-enabled fraud has been analyzed through a single lens: financial loss to the victim. That lens is no longer sufficient. The FATF has now formally and explicitly recognized cyber-enabled fraud as a money-laundering, terrorist-financing, and proliferation-financing risk in its own right, not an indirect concern, but a named category in its own typology paper. Its companion publication, the July 2025 Comprehensive Update on Terrorist Financing Risks, goes further: it documents a structural shift away from large, centrally-organized terrorist financing flows and toward decentralized, self-financed cells and lone actors who rely on "microfinancing strategies drawn from licit sources and petty crimes, as well as technology-enabled methods, including gaming and social media features." The report identifies trade-enabled fraud through social media and informal crowdfunding as standalone typology chapters —the same channels that now generate the bulk of Pakistan's own fraud complaints.

The financing pattern terrorist financiers increasingly prefer small, frequent, decentralized, hard-to-trace, is structurally identical to the proceeds a phishing campaign, a fake investment app, or a romance scam generates. Where a conventional AML system is tuned to flag a single large, unusual transfer, this typology is engineered to defeat exactly that kind of monitoring. It moves in volume, not in size.

Why Pakistan Cannot Treat This as a Distant Risk

Pakistan's own record gives this risk a concrete, rather than theoretical, shape. The country was placed on the FATF's grey list three separate times 2008–2010, 2012–2015, and again from June 2018 until October 2022 each time explicitly for terrorist-financing deficiencies. Exiting the 2018 listing required a combined 34-point action plan (27 points from 2018, plus 7 added in 2021) and a formal FATF/Asia Pacific Group on-site verification visit in September 2022. Yet even after its October 2022 removal, the APG's own follow-up assessment rated Pakistan's effectiveness as "low" on 10 of the 11 international AML/CFT outcomes it measures, despite Pakistan being technically

compliant or largely compliant on 38 of 40 FATF Recommendations. In other words: Pakistan can pass the paperwork test and still fail the operational test—precisely the gap FATF's 2025 global report says now exists in 69% of jurisdictions worldwide when it comes to investigating, prosecuting, and convicting terrorist-financing cases.

That operational gap is visible in Pakistan's cyber-crime enforcement data specifically, not just its terrorist-financing data. Figures presented in the National Assembly show that the NCCIA received 523,749 cybercrime complaints between 2023 and 2026 but secured only 199 convictions, a conviction rate of approximately 0.038%. Year by year, the trend has worsened even as complaints have stayed high: 92 convictions against 134,710 complaints in 2023; 60 convictions against 161,828 complaints in 2024; 39 convictions against 157,465 complaints in 2025; and just 8 convictions against 77,023 complaints in the first part of 2026. The predecessor FIA Cybercrime Wing's longer record is similar: over 639,000 complaints since 2020 produced only 222 convictions, a rate of 3.16%. An environment where fewer than four in ten thousand cybercrime complaints end in conviction is, by definition, an environment where illicit proceeds fraud-derived or otherwise can move with very little fear of consequence. That is the same permissive environment terrorist financing requires.



Cyber-enabled fraud is rising sharply across South Asia, and rising fraud volumes regionally widen the pool of illicit, low-trace funds moving through porous cross-border financial and informal corridors that have historically also carried terrorist-financing flows into and out of Pakistan."

Pakistan's security establishment has already documented technology-enabled financing channels reaching active militant groups. Intelligence briefings described cross-border handlers using illegal telecommunications spectrum to direct financial transactions to the band outfits. Separately, NACTA's own risk-rating exercise found that 6.75% of Pakistan's non-profit organizations (NPOs) carry a high terror-financing risk rating and 43.64% carry a medium rating part of why NACTA has banned few organizations, and why Pakistan froze several unregistered bank accounts under the 2015 National Action Plan. These are not digital-fraud cases but they establish, beyond doubt, that the technical capability, the cross-border handler networks, and the institutional appetite to route funds to designated terrorist organizations through non-traditional channels risk can be raised more in Pakistan, if counter measures are not implemented correctly. The remaining question for digital financial institutions is whether fraud-proceed laundering pipelines mule accounts, unlicensed crypto off-ramps, social-media crowdfunding are being or could be tapped by the same networks.

That question is not abstract. In one of the clearest illustrations of the underlying vulnerability, the FIA built a case alleging that a major international cryptocurrency exchange's platform was used to defraud more than 100,000 Pakistanis of over \$100 million through fake trading schemes funds that moved through largely unregulated, pseudonymous, borderless virtual-asset rails with no licensed Pakistani AML/CFT gatekeeper in the chain. It is exactly this class of exposure that the Pakistan Virtual Assets Ordinance, 2025, and the new Pakistan Virtual Assets Regulatory Authority (PVARA) are designed to close, by requiring virtual asset service providers to be licensed and supervised under SBP-aligned AML/CFT rules rather than operating, as much of the sector has to date, through offshore wallets and informal exchanges.

Red Flags Digital Financial Institutions Should Treat as Converged Risk

FATF's typology work and Pakistan's own enforcement record point to a consistent set of indicators that fraud-control and AML/CFT teams should monitor jointly rather than separately:

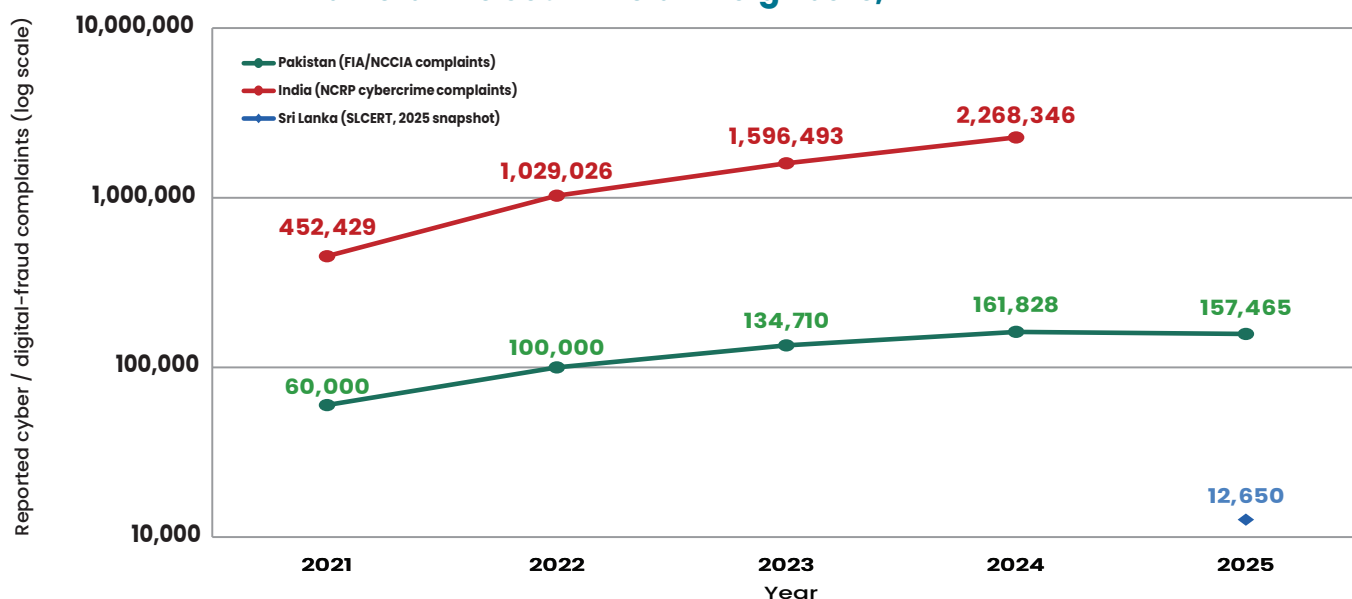
- High-frequency, low-value peer-to-peer transfers structured just beneath reporting thresholds, fanning out from a single source account to multiple recipients in a short window.
- Mule-account chains that terminate in rapid cash withdrawal or onward transfer near border regions or areas with a documented militant presence.
- Social-media or messaging-app crowdfunding campaigns using vague humanitarian or religious framing, consistent with FATF's "informal crowd-funding" and "trade-enabled fraud through social media" typologies.

- Rapid conversion of fraud proceeds into virtual assets and off-ramping through unlicensed or offshore platforms, rather than SBP/PVARA-licensed VASPs which is currently under implementation phase.
- Donation mechanisms (digital collection boxes, QR codes, NPO accounts) tied to entities that fall within NACTA's medium- or high-risk NPO categories, or that resemble previously banned organizations operating under a new name.
- Accounts opened through e-KYC using synthetic or stolen identities that subsequently receive irregular inbound transfers from multiple unrelated fraud-victim accounts, before rapid onward movement.

None of these indicators, on its own, proves a terrorist-financing link the overwhelming majority of fraud proceeds are laundered for ordinary criminal profit. The point is structural, not accusatory: Pakistan's digital financial institutions are now generating, in real time, exactly the kind of decentralized, low-trace transactional data that FATF says terrorist financiers are migrating toward globally, inside a domestic enforcement environment that secures a conviction in roughly 4 of every 10,000 cybercrime complaints. Closing that gap should not be just reducing fraud losses, rather it should be treated as a national-security priority by FIs, and their regulators alike.

This pattern is also not unique to Pakistan, which is part of why it deserves regional attention rather than purely domestic remediation. Cyber-enabled fraud is rising sharply across South Asia, and rising fraud volumes regionally widen the pool of illicit, low-trace funds moving through porous cross-border financial and informal corridors that have historically also carried terrorist-financing flows into and out of Pakistan.

Digital Fraud & Cybercrime Complaints: Pakistan vs South Asian Neighbors, 2021-2025



Pakistan growth: 2022 to 2025 approx. +57% cumulative (with a 35% surge reported by NCCIA for 2025 alone; banking fraud specifically up 62%).

India growth: 2021 to 2024 approx. +401% cumulative (NCRP), driven by UPI-linked scams & 'digital arrest' fraud (+210% in 2024 alone).

Bangladesh: no centralised annual complaint count is published; CCAF survey work shows financial-loss share of cybercrime victims rising. Sri Lanka:

SLCERT logged 12,650+ complaints in 2025, a sharp rise versus prior years (no comparable pre-2025 published baseline).

Sources: FIA Annual Administration Reports; NCCIA; India NCRP/14C (Lok Sabha disclosures, Dec 2025); Sri Lanka CERT (2025).

Note: Absolute counts are not population-adjusted - India's population (~1.45bn) is ~6x Pakistan's (~245m); use trend direction, not raw scale, for comparison.

Figure 3: Digital Fraud & Cybercrime Complaints — Pakistan vs. South Asian Neighbors, 2021-2025

India's National Cybercrime Reporting Portal recorded complaints rising from 452,429 in 2021 to 2,268,346 in 2024 a cumulative increase of over 400% driven substantially by UPI-linked scams and so-called "digital arrest" fraud, which alone grew an estimated 210% in 2024. Sri Lanka's CERT logged over 12,650 complaints in 2025, a sharp rise versus prior years. Bangladesh has no single, centralized annual complaint count, but independent survey work by the Cyber Crime Awareness Foundation shows a rising share of cybercrime victims reporting direct financial loss. None of this is offered as equivalence; each country's institutional capacity and terrorist-financing risk profile differs. However, it underlines that the underlying criminal infrastructure (mule networks, crypto off-ramps, social-engineering scripts) is increasingly regional, and that any Pakistani institution's CFT controls that stop at the country's border are, by definition, incomplete.

What This Means in Practice

FATF's own recommended response to cyber-enabled fraud payment transparency mechanisms such as confirmation-of-payee, faster cross-border asset-freezing and non-conviction-based confiscation tools, closing gaps in virtual-asset regulation, and stronger beneficial-ownership transparency to unmask the shell companies fraud rings use to hide proceeds, should be read by Pakistani digital financial institutions as counter-terrorist-financing measures, not merely as fraud-loss-reduction measures. The two are now, in FATF's own framing, the same control set.

AML/CFT Challenges in Instant Digital Payments

Instant digital payments have revolutionized financial access remote account opening, instant transfers, QR payments, and round-the-clock service but they have also compressed the window available for manual AML/CFT intervention to nearly zero. Digital onboarding and remote e-KYC, while efficient, create openings for stolen identities, forged documents, and increasingly convincing synthetic identities built with generative AI. Real-time transaction monitoring is no longer a nice-to-have; it is the only practical control left once funds can move and settle in seconds through RAAST.

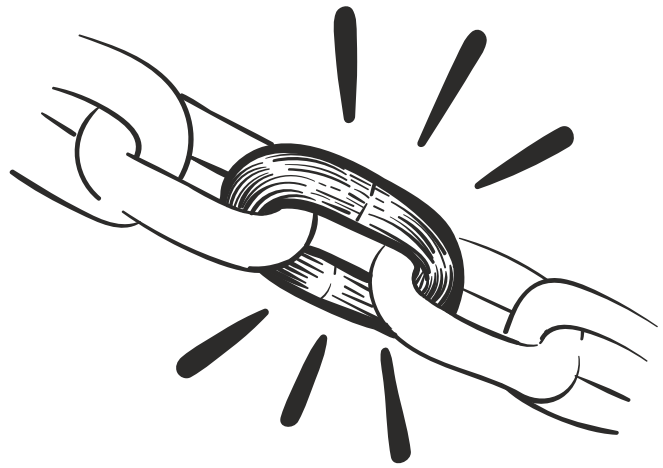


The clearest institutional lesson is that fraud prevention, cybersecurity, and AML/CFT compliance can no longer be run as three separate functions within a FI."

Money-mule accounts and complex ownership structures remain the connective tissue between fraud and money laundering and, potentially terrorist financing. Cross-border digital payments add sanctions-screening and high-risk-jurisdiction complexity on top. The clearest institutional lesson is that fraud prevention, cybersecurity, and AML/CFT compliance can no longer be run as three separate functions within a FI.

Pakistan's financial institutions need a single, integrated financial-crime framework that combines real-time fraud detection, transaction monitoring, digital-identity verification, and AML/CFT screening because the criminal flows themselves no longer respect those internal departmental boundaries. This can only be done by creating synergy between Fraud Dept. teams and Compliance AML Teams within FIs. Discussions on the cases between teams, sharing of findings can lead for a better Suspicious report generations and instant action against culprits.

Regulatory Technology (RegTech) and Supervisory Technology (SupTech) are the practical instruments for closing this gap: automated e-KYC, biometric and liveness verification, AI-driven sanctions and PEP screening, behavioral analytics, and machine-learning-based supervisory reporting that lets SBP, the SECP, and the Financial Monitoring Unit (FMU) assess emerging typologies, including the fraud-to-terror-financing convergence described above, far earlier than periodic on-site inspections fruitfulness.



Collaboration: The Missing Link

Cyber-enabled financial crime does not respect institutional boundaries, and neither does its potential terrorist-financing endpoint. Criminals and, per FATF's 2025 findings, an increasing number of self-financed extremist actors exploit weaknesses across banks, EMIs, telecom networks, payment systems, social media platforms, and international financial channels simultaneously. No single Pakistani institution holds enough information to see the full picture alone.

Effective prevention requires structured collaboration among the NCCIA, SBP, the SECP, the FMU, NACTA's CFT Wing, the Pakistan Telecommunication Authority (PTA), NADRA, commercial banks, Digital banks, EMIs, Fintech companies, and telecom operators. NACTA's CFT Wing already performs much of the terrorist-financing-specific risk assessment and federal-provincial coordination function; what is missing is a routine, two-way information bridge between that CFT-specific machinery and the fraud and cybersecurity teams inside FIs, who are often the first to see the transactional patterns NACTA and the FMU need. Shared fraud-

intelligence databases, real-time account-freezing mechanisms tied to PVARA-licensed virtual-asset platforms, and joint public-private incident response would close much of the gap so far described.



Cyber-enabled fraud should be reclassified inside Pakistan's financial institutions and regulatory bodies, from a compliance obligation and a customer-protection issue into a national resilience imperative that sits alongside counter-terrorism policy".

Sustainable Growth Strategies for FIs

Pakistan's FIs including Digital Financial Service industry's long-term health depends on diversifying beyond pure payment-transaction revenue; merchant acquisition across retail, transport, and SME segments; embedded finance integrated into e-commerce, ride-hailing, and logistics platforms; alternative credit scoring built on transaction-history data for underserved borrowers; and API banking / Banking-as-a-Service (BaaS) models that let licensed institutions extend regulated infrastructure to fintech startup partners. None of this growth is inconsistent with the risk, in fact, an EMI sector built on diversified, transparent, well-documented revenue streams is structurally easier to supervise than one dependent on opaque, high-volume micro-transaction flows alone.

Islamic Fintech: Opportunity with a Governance Caveat

Pakistan's demand for Shariah-compliant digital finance Islamic digital wallets, Murabaha- and Musharakah-based financing, digital Takaful, and Islamic crowdfunding represents a genuine growth opportunity. Digital Zakat and Waqf platforms in particular can make charitable giving more transparent and efficient than the cash-collection-box model NACTA has already flagged as a historical NPO-abuse channel. That is precisely why these platforms need Shariah governance and AML/CFT controls built in from day one, rather than added retroactively: a digital Zakat platform with weak beneficiary verification simply digitizes the same NPO-diversion risk NACTA's describes in its publications, at greater speed and scale. Strong Shariah governance, AAOIFI-aligned product approval, and routine digital Shariah audits should be treated as AML/CFT controls, not separate compliance tracks.

Consumer Awareness: The Strongest Firewall

No technology stack fully substitutes for an informed customer. Criminals succeed most often not because security systems fail but because individuals are persuaded to disclose an OTP, click a link, or trust a

fake customer-service call. Financial and digital literacy campaigns delivered through schools, universities, workplaces, television, and financial institutions themselves remain the cheapest and most scalable control available to Pakistan's regulators. Given the argument above, these campaigns now carry a second, less obvious payoff: every consumer who avoids becoming a fraud victim is also one less innocent contributor to the pool of illicit funds that can be diverted toward financing violence.

The Road Ahead: From Compliance Obligation to National Resilience Imperative

Pakistan has built multipronged digital-payments infrastructure in a short period: RAAST, the EMI framework, NADRA's digital identity system, PRISM+, and now upcoming implementation on PVARA and the Virtual Assets Ordinance, 2025. Digital channels carry 92% of retail payment volume; annual digital transactions have roughly magnified since 2021. These are genuine achievements, and they should not be undersold.

Although the proportionate growth in cyber fraud cases is less than the growth in the use cases of digital finance, still there exist a glaring need in Pakistan to create awareness among the masses about its growing instances in addition to segmenting the institutional capability and support. FATF's own global research finds that 69% of assessed jurisdictions have major or structural deficiencies in investigating, prosecuting, and convicting terrorist-financing cases, and that terrorist financiers are migrating toward exactly the decentralized, low-value, technology-enabled funding patterns that digital scams generate. Pakistan's own data a three-time FATF grey-listing history rooted in terrorist-financing deficiencies, a 0.038% cybercrime conviction rate against 523,749 NCCIA complaints since 2023, documented technology-enabled financing channels reaching banned organizations, and a \$100 million unregulated crypto-fraud case affecting over 100,000 citizens shows this is not an imported warning. It is a description of present conditions.

Cyber-enabled fraud should therefore be reclassified inside Pakistan's financial institutions and regulatory bodies, from a compliance obligation and a customer-protection issue into a national resilience imperative that sits alongside counter-terrorism policy. The institutions that integrate fraud detection, AML/CFT screening, and CFT-specific typology awareness into one framework supported by RegTech, SupTech, NACTA-FMU-bank information sharing, and a digital-identity system that closes rather than widens the e-KYC gap will be the ones equipped to manage this risk. Pakistan's transition from a cash-based to a digitally connected financial ecosystem is a milestone which is irreversible. Whether that transition strengthens or undermines the country's security will depend on how quickly its AML/CFT framework, cybersecurity capability, and prosecutorial capacity can close the gap. ■