



REPUBLIC OF KENYA

PROPOSED REVISIONS TO THE DRAFT NATIONAL PAYMENT SYSTEM POLICY, 2026

INSTITUTION: FORTIFY TECHNOLOGY LIMITED (WWW.FORTIFY.COM)

DATE: 8 OCTOBER 2026

S/No	Section no.	Provisions of the section*	Rationale for revision Recommendation	Proposed revision**
1	Section 2.6, after item v)	Section 2.6 identifies gaps in resilience, real-time supervisory visibility, cybersecurity and consumer protection. Fraud appears within the cybersecurity and consumer-protection discussion, but fraud and financial crime are not identified as a distinct NPS gap.	Payment fraud, scams, account takeover, mule-account activity and AML/CFT/CPF risks cut across cybersecurity, consumer protection, market integrity and payment operations. Treating them only as components of other risks can understate the need for coordinated detection, monitoring, investigation, reporting and sector-wide response. A distinct gap statement would create a clearer policy basis for the interventions and implementation measures that follow.	Insert a new item after item v) and renumber the subsequent items: “vi) Fraud and Financial Crime Management Gaps: The speed, scale and increasing interoperability of digital payments heighten exposure to payment fraud, scams, account takeover, mule-account activity, money laundering, terrorist financing and proliferation financing. Institutions operate with differing data, monitoring, screening, investigation and reporting capabilities, limiting consistent detection and coordinated response across the NPS. This Policy therefore provides for a coordinated, risk-based fraud and financial crime management framework across the NPS, including appropriate transaction monitoring, compliance screening, investigation and case management, standardised fraud reporting, control testing and secure information-sharing mechanisms, subject to applicable data-protection and confidentiality requirements.”
2	Section 3.4.3, Intervention 3	Intervention 3, “Strengthen Risk Management Practices”, currently provides for: i) development and implementation of risk management frameworks; and ii) a national incident response and coordination mechanism for systemic threats.	The intervention is broad and does not translate the Policy issue of financial crime into specific operational outcomes. The NPS would benefit from a clear expectation that PSPs and PSOs maintain risk-based fraud and financial-crime controls that operate at the speed of modern payment services and are periodically tested for effectiveness.	Revise Intervention 3 to read: “Intervention 3: Strengthen Fraud and Financial Crime Risk Management Practices Strategies The Government will undertake the following under this initiative in the payment ecosystem: i) Develop and implement risk-based fraud and financial crime management frameworks for PSPs and PSOs. ii) Establish proportionate requirements for transaction monitoring, fraud detection, AML/CFT/CPF screening, investigation, escalation and regulatory reporting. iii) Require periodic testing of the design and operating effectiveness of material fraud and financial-crime controls, including data quality, rules or models, alert handling and case management.

S/No	Section no.	Provisions of the section*	Rationale for revision Recommendation	Proposed revision**
				iv) Promote real-time or near real-time controls for instant or irrevocable payments where proportionate to the risk. v) Establish a national incident response and coordination mechanism for material fraud, financial-crime and systemic threats.”
3	Section 3.4.3, Intervention 5	Intervention 5, “Strengthen Collaboration and Information Sharing”, currently focuses on public-private partnerships for risk management and coordination with regional and international regulators on cross-border cyber and operational risks.	Fraud frequently moves across banks, PSPs, mobile-money providers, telecommunications channels and third-party platforms. Effective prevention requires timely and controlled sharing of actionable risk indicators and typologies, not only regulator-to-regulator coordination. The Policy should establish a clear objective for a national fraud and payment-risk intelligence framework with privacy, confidentiality and purpose-limitation safeguards.	Add the following strategies under Intervention 5: “iii) Establish a secure national payment fraud and financial-crime intelligence-sharing framework involving relevant regulators, financial institutions, PSPs, PSOs, telecommunications providers, law-enforcement agencies and approved technology or RegTech providers. iv) Develop common standards and governance for sharing fraud indicators, mule-account intelligence, compromised identifiers, device or channel indicators and emerging typologies, subject to data-protection, confidentiality, information-security and purpose-limitation requirements. v) Promote aggregated and anonymised sector reporting on fraud trends, losses, recovery outcomes and emerging typologies to strengthen risk-based supervision and industry response.”
4	Section 3.5.3, Intervention 1(ii)	The Policy proposes to “Establish liability and fraud prevention frameworks” as part of strengthening consumer protection within the payment ecosystem.	The proposal is directionally appropriate but does not specify preventive measures suited to instant and increasingly irrevocable payments. Consumer protection is stronger where institutions can identify suspicious or misdirected payments before execution, apply proportionate warnings or step-up controls, and support timely recall and recovery after an incident.	Revise item ii) to read: “ii) Establish liability and fraud prevention frameworks that promote risk-based payment pre-validation, beneficiary verification, strong customer authentication, transaction warnings and step-up controls, appropriate transaction holds, and timely recall or recovery procedures, with clear allocation of responsibilities for unauthorised transactions and payment scams.”
5	Section 3.3.3, Intervention 2	Intervention 2, “Promote financial innovation in the payment ecosystem”, provides for regulatory collaboration, sandboxes, licensing requirements and supervisory guidelines for emerging areas. The Policy separately defines RegTech but does not expressly include RegTech or fraud-prevention technology within its innovation strategies.	RegTech and fraud-prevention technology can help institutions meet regulatory obligations at payment speed while improving auditability, supervisory reporting and control effectiveness. Explicit policy recognition would encourage responsible adoption, provide a basis for standards around interoperability and oversight, and clarify the role of specialised technology providers supporting regulated institutions.	Add the following strategy under Intervention 2: “v) Promote responsible adoption of regulatory technology, fraud-prevention and compliance technology to strengthen monitoring, screening, investigation, reporting and supervisory visibility across the payment ecosystem, and develop proportionate standards for interoperability, auditability, data protection, resilience and oversight of material technology service providers.”
6	Chapter 5 and Annexure 1, Objectives 4 and 5	Chapter 5 provides for annual monitoring and evaluation plans covering activities, timelines, outcomes, data collection and reporting. Annexure 1 implements the risk-management and consumer-protection objectives but does not set specific fraud or financial-crime performance measures.	The Policy will be more effective if implementation can be measured beyond adoption of frameworks. Common indicators would help Government and regulators assess whether fraud and financial-crime controls are improving outcomes, identify sector weaknesses and evaluate the effectiveness of information-sharing and supervisory initiatives over time.	Add to the Monitoring and Evaluation Framework and Annexure 1: “Implementation indicators for Objectives 4 and 5 shall include measurable fraud and financial-crime outcomes, including adoption of standardised fraud reporting, trends in attempted and successful fraud and losses, recovery

S/No	Section no.	Provisions of the section*	Rationale for revision Recommendation	Proposed revision**
				outcomes, implementation and testing of transaction-monitoring and screening controls, participation in approved information-sharing arrangements, and timeliness of material incident reporting. Sector-level publication shall use aggregated or anonymised information where necessary to protect customers, investigations and confidential supervisory information.”

*Provide text on exact wording of the provision in the section of the draft policy

** Provide the exact wording of how the proposed revision to the section is proposed to read.

- a) **Briefly describe your role in this framework:** Fortify Technology Limited is a Kenya-based RegTech and fraud-risk technology provider supporting financial institutions and payment service providers with real-time payment fraud detection, transaction monitoring, AML/CFT/CPF screening, investigation and case management, and compliance reporting.
- b) **Additional remarks:** Fortify supports the objectives of the Draft National Payment System Policy. These comments focus on strengthening fraud risk management, financial-crime controls, data and information sharing, consumer protection and the role of technology providers. We recommend that fraud and financial crime be treated as a distinct and measurable policy pillar alongside cybersecurity, operational resilience and consumer protection, with proportionate regulation and appropriate data-protection safeguards.