



REPUBLIC OF KENYA

PROPOSED NATIONAL PAYMENT SYSTEM BILL, 2026

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

DATE: 8 OCTOBER 2026

S/No	Clause & Subclause	Provisions of the Clause*	Proposed Revision**	Rationale for the revision/ Recommendation
1	Clause 2; Clause 4(1)(o); Clause 9; First Schedule	Clause 2 defines “ancillary services” to include technical, operational, data processing, authentication, security and fraud prevention services. Clause 4(1)(o) applies the Act to a person that engages in ancillary services supporting a payment system or payment service. The First Schedule, however, contains licence categories only for payment service providers and payment system operators.	Insert in Clause 2: “regulatory technology (RegTech)” means technology used to improve regulatory compliance, monitoring, screening, risk management and reporting processes in the financial sector. Insert after Clause 9(7): “(8) A person that provides ancillary services only, including technical, operational, data processing, authentication, security, fraud prevention or regulatory technology services, shall not by reason only of providing those services be required to obtain a licence under section 5 or section 6. (9) Notwithstanding subsection (8), the Central Bank may, where an ancillary service is material to the safety, integrity or continuity of the national payment system, designate the provider as a critical ancillary service provider and prescribe proportionate registration, risk-management, audit, information-security and supervisory requirements.”	The Bill brings fraud-prevention and other ancillary providers within its application but does not state whether they require a licence or how they are supervised. This creates regulatory uncertainty for RegTech, fraud and security providers. A proportionate critical-provider framework would recognise their role without treating non-funds-handling technology providers as PSPs or PSOs, while preserving CBK oversight where a third party is material to payment-system safety or integrity.
2	Clause 19	Clause 19(1) requires persons subject to the Act to comply with the Proceeds of Crime and Anti-Money Laundering Act in relation to AML/CFT/CPF. Clause 19(2) gives CBK inspection, surveillance, sanction, rule-making and information-sharing powers.	Insert after Clause 19(3): “(4) Every payment service provider and payment system operator shall establish and maintain risk-based systems and controls, proportionate to the nature, scale and complexity of its activities, to give operational effect to subsection (1), including: (a) customer and beneficial-owner risk assessment; (b) screening against applicable sanctions and targeted financial sanctions requirements; (c) identification and enhanced-risk treatment of politically exposed persons and other higher-risk relationships as required by law; (d) ongoing transaction monitoring; (e) identification, investigation and escalation of unusual or suspicious activity; (f) reporting in accordance with applicable law; and (g) retention of auditable evidence of decisions and actions.”	The POCAMLA cross-reference establishes the legal obligation, but the Bill does not expressly require payment institutions to maintain the operational screening, monitoring and investigation capability needed to discharge it. The proposed wording avoids duplicating POCAMLA while making clear that compliance must be supported by effective systems, controls and auditable evidence.
3	New Clause 27A	The Bill addresses market conduct, material incidents, payment traceability and specific payment-fraud controls, but it does not establish an institution-wide fraud risk management duty for PSPs and PSOs.	Insert after Clause 27: “27A. Fraud risk management. (1) Each payment service provider and payment system operator shall establish, implement and maintain a documented, risk-based fraud risk	The Bill contains discrete fraud provisions, particularly in Part X, but does not create a clear end-to-end fraud-management obligation. A technology-neutral statutory duty would make fraud prevention and detection a core operating requirement

S/No	Clause & Subclause	Provisions of the Clause*	Proposed Revision**	Rationale for the revision/ Recommendation
			management framework proportionate to the nature, scale, complexity and speed of the services it provides. (2) The framework shall cover prevention, customer authentication, transaction monitoring, detection, investigation, response, recovery, customer notification, regulatory reporting, control testing and continuous improvement. (3) Where a service supports instant or irrevocable payments, fraud controls shall operate in real time or near real time where reasonably practicable and proportionate to the risk. (4) The Central Bank may prescribe minimum governance, data, control-testing, rule or model validation, investigation and reporting requirements.”	rather than only a payment-traceability, consumer-remediation or post-incident issue.
4	Clause 26	Clause 26 allows CBK to collect data and information necessary for supervision and to require PSPs and PSOs to submit statistical and other periodic returns.	Insert after Clause 26(5): “(6) Without prejudice to reporting obligations under the Proceeds of Crime and Anti-Money Laundering Act, the Central Bank shall prescribe a common taxonomy and periodic reporting framework for payment fraud, including attempted and successful fraud, losses, payment channel and type, fraud typology, unauthorised transactions, payment scams, account takeover, mule-account indicators, recovery outcomes and such other information as the Central Bank may prescribe. (7) The Central Bank may publish aggregated or anonymised sector statistics, trends and typologies derived from information collected under subsection (6).”	Clause 26 provides broad information-collection powers and Clause 33 addresses material events, but neither establishes comparable sector-wide fraud reporting. A common taxonomy would improve supervisory visibility, enable trend and typology analysis, support earlier intervention and provide institutions with better sector intelligence without requiring disclosure of customer-level information.
5	Clauses 51(3) and 53(f)	Clause 51(3) requires beneficiary PSPs to maintain appropriate systems and controls to mitigate misdirected payments and payment fraud. Clause 53(f) permits rules or standards on measures for preventing and addressing misdirected payments and payment fraud.	Revise Clause 51(3) to read: “(3) Each beneficiary payment service provider shall maintain appropriate systems and controls to mitigate the risk of misdirected payments, payment fraud and payment scams, including risk-based payment pre-validation or beneficiary verification where prescribed by the Central Bank.” Revise Clause 53(f) to read: “(f) measures for preventing and addressing misdirected payments, payment fraud and payment scams, including, where appropriate, payment pre-validation, beneficiary verification, risk-based warnings, transaction holds or step-up controls, and procedures for recall or recovery;”	The existing clauses recognise payment fraud but leave key preventive controls implicit. For fast or irrevocable payments, proportionate pre-payment controls can identify mismatches and elevated risk before funds leave the payer. The proposed wording preserves CBK discretion to determine where these measures are appropriate.
6	Clauses 54 and 55	Clauses 54 and 55 allow CBK to cooperate and share information with public agencies, monetary authorities, financial regulators, fiscal or tax agencies and fraud-investigation agencies.	Insert after Clause 54(2): “(3) The Central Bank may establish, approve or facilitate secure arrangements for sharing fraud and payment-risk intelligence among payment service providers, payment system operators, financial institutions, telecommunications providers, relevant public agencies and approved service providers, subject to applicable data-protection, confidentiality, purpose-limitation and information-security requirements. (4) Arrangements under subsection (3) may provide for the sharing of indicators relating to compromised identifiers, mule accounts, fraudulent	The current provisions primarily facilitate information sharing involving CBK and public or foreign authorities. They do not expressly provide a basis for controlled industry fraud-intelligence sharing across the institutions and channels through which payment fraud can move. A safeguarded framework would support earlier detection of repeat attack patterns and mule networks while preserving privacy and confidentiality.

S/No	Clause & Subclause	Provisions of the Clause*	Proposed Revision**	Rationale for the revision/ Recommendation
			devices or channels, transaction patterns and emerging fraud typologies, and shall include safeguards against use of shared information for unrelated purposes.”	
7	Clause 35(4)	Clause 35 requires annual system audits and defines a system audit as an independent evaluation of operational and management systems for compliance, safeguarding assets, data integrity, efficiency, risks and weaknesses.	Revise the definition of “system audit” in Clause 35(4) by adding at the end: “and shall include, where applicable, assessment of the design and operating effectiveness of cybersecurity controls, fraud prevention and detection controls, AML/CFT/CPF screening and transaction-monitoring controls, data quality and completeness, rule or model governance, alert and case-management processes, third-party controls, incident response and compliance reporting.”	The existing definition is broad but does not expressly require auditors to test whether fraud and financial-crime controls operate effectively. Adding these areas would strengthen evidence of control effectiveness and improve the quality of information available to both institutions and CBK when assessing monitoring, screening and investigation controls.
8	Clause 76(2)	Clause 76(2) expressly lists matters for which regulations may be made, including supervision, data sharing, outsourcing, material disclosure, interoperability, cybersecurity, open finance and market conduct. Fraud risk management, compliance screening and RegTech are not expressly listed.	Insert after Clause 76(2)(q): “(r) fraud risk management and fraud reporting; (s) AML/CFT/CPF technology controls, screening and transaction monitoring; (t) payment pre-validation, beneficiary verification and customer authentication; (u) fraud and payment-risk information-sharing arrangements; and (v) the use and oversight of regulatory technology and critical ancillary service providers.”	The Bill is principles-based and leaves substantial operational detail to regulations. Expressly including these matters would give a clear legal foundation for proportionate and adaptable standards on fraud prevention, financial-crime controls and specialised technology providers.

*Provide text on exact wording of the provision in the proposed clause or clauses

** Provide the exact wording of how the proposed bill or clause 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 Proposed National Payment System Bill, 2026. These comments focus on strengthening fraud risk management, financial-crime controls, payment transparency and traceability, industry information sharing, consumer protection, and the proportionate treatment of RegTech and fraud-prevention technology providers. We recommend that the Bill provide a clear legal foundation for risk-based fraud prevention, AML/CFT/CPF screening and transaction monitoring, measurable control effectiveness, secure fraud-intelligence sharing, and proportionate oversight of critical ancillary service providers.