

Draft Money & Payment Services Policy

[Memorandum of Policy]

Table of Contents

1. Introduction	1
2. Vision	3
3. Purpose, Objectives and Policy Goals	4
4. Guiding Principles	6
5. Rationale for Replacing the Money-Changing and Remittance Business Act 2009	7
6. National Electronic Transactions Policy Instruments	9
7. Legislative Harmonization Framework	11
8. Key Stakeholders	12
8. Implementation Roadmap	14
9. Risks and Mitigation Strategies	17
10. Conclusion	19
11. Glossary	20

1. Introduction

The Money-Changing and Remittance Businesses Act 2009 (hereinafter, the “Act” or “MCRB Act”) was enacted to regulate two narrowly defined services—cash-based foreign-exchange kiosks (“money-changing business”) and manual telegraphic transfers (“remittance business”)—in an era when digital finance was in its infancy. Today, however, global payment landscapes are dominated by electronic-money issuers, mobile-wallet platforms, real-time gross-settlement (RTGS) systems, and online peer-to-peer remittance services—none of which fall within the Act’s definitions or licensing framework. As a result, local fintech startups have been operating under improvised licence conditions, stretching the FSC’s supervisory remit and creating legal uncertainty for both regulators and market entrants.

The Act’s two licence classes (Part II) and capital requirements were calibrated for brick-and-mortar operators, with fixed fees and no tiering for low-value or high-volume digital services. Sections 11–12 empower the Financial Supervisory Commission (FSC) to inspect cash-handling premises and issue directives, but offer no authority to audit electronic records, mandate real-time transaction reporting, or oversee algorithmic controls in payment-system software. Consumer-protection measures—fund-segregation and dispute-resolution provisions in Part III—presume trust-account ledgers maintained by physical licensees, providing no rules for safeguarding e-wallet float or resolving digital-channel disputes. Meanwhile, AML/CFT obligations (Sections 13–14) envisage manual KYC checks and cash-transaction monitoring, omitting FATF’s e-KYC guidance, sanctions-screening protocols, and continuous surveillance standards now deemed essential for mitigating digital-payment risks.

And even from a fundamental standpoint, the MCRB Act does not account for modern fintech and digital channels—**mobile wallets, online money transfer platforms, and electronic money** are outside its scope. These legislative gaps create uncertainty around the regulatory treatment of innovative services, impede the introduction of cost-saving digital remittance channels, and limit the country's ability to leverage new technologies.

These gaps also carry real costs. Pacific remittance corridors rank among the most expensive globally—averaging 9.1 % per transaction in Q4 2022 versus a global average of 6.26 %—and are over three times the UN SDG target of 3 %.¹ High fees disproportionately burden remote and low-income communities in the Cook Islands, where diaspora remittances are a vital lifeline. At the same time, outdated AML/CFT frameworks threaten correspondent-bank relationships, as international partners de-risk jurisdictions with legacy regimes—a dynamic that can further restrict access to global payment rails.

To address these challenges, this memorandum seeks Cabinet's approval to draft comprehensive amendments that will:

1. **Broaden statutory scope** by redefining “money services” to include electronic-money institutions, payment-system operators, mobile-wallet providers, and real-time remittance platforms.
2. **Introduce a risk-based, tiered licensing regime** with proportional fees, capital thresholds keyed to transaction volumes (including retaining no capital requirements for small local entities) and streamlined authorizations for low-value services.
3. **Enhance FSC supervisory powers** by empowering delegated rule-making, mandating real-time transaction reporting, and granting authority to audit electronic records and algorithmic-control mechanisms.
4. **Embed robust consumer safeguards**—including mandatory segregation of e-wallet float, clear digital-channel disclosures, and electronic dispute-resolution processes.
5. **Align AML/CFT standards** fully with FATF's e-KYC recommendations, sanctions-screening obligations, and continuous transaction-monitoring protocols.

The core objective of the proposed amendments is to establish clear, risk-proportionate rules that bring new digital remittance services under appropriate supervision while enabling innovation. By updating definitions, licensing categories, and oversight powers, the reforms will **remove outdated restrictions** that hinder fintech adoption, **reduce ambiguity** in applying AML/CFT controls, and **open the market** to safe, efficient digital providers. The updated framework will be **grounded in international standards** – including the Financial Action Task Force (FATF) recommendations that all money transfer and currency exchange providers be licensed and monitored – and informed by regional benchmarks in digital payments.

¹ <https://remittanceprices.worldbank.org/>

These reforms will future-proof the Cook Islands' "Money Services" framework—reducing remittance costs, expanding financial inclusion in remote communities, and safeguarding the integrity and stability of digital payment ecosystems.

2. Vision

This vision imagines a modern Cook Islands where individuals, businesses, and diaspora communities can seamlessly exchange and send money with confidence. The remittance and money-changing sector will be **vibrant, trustworthy, and accessible**, driving economic resilience and supporting livelihoods. To realize this vision, the policy establishes a forward-looking framework for the MCRB Act that enables fintech growth while safeguarding financial integrity.

The policy will:

- **Enable digital innovation in remittances:** Introduce legal recognition for electronic money and digital remittance platforms, allowing services like mobile wallets and online transfers to operate under clear rules. This will remove barriers to fintech adoption and lower transaction costs.
- **Promote financial inclusion and competition:** Encourage new market entrants (including fintech startups and non-bank operators) to increase competition and reach underserved communities. A more competitive remittance market is expected to reduce fees and extend services to remote islands and unbanked populations.
- **Strengthen consumer protection and trust:** Build public confidence through robust consumer safeguards – mandating transparency in fees, data privacy, and dispute resolution for remittance services. A **trustmark or accreditation framework** for reliable providers may be introduced to signal safety and security.
- **Enhance compliance and security:** Align with international AML/CFT standards by tightening licensing requirements and supervision of money transfer operators, thus mitigating risks of money laundering, terrorist financing, and fraud. Digital ID and e-KYC (electronic Know-Your-Customer) systems will be leveraged where possible to improve compliance efficiency.
- **Support integration with payment infrastructure:** Prepare the regulatory ground for future payment system innovations, such as a national real-time gross settlement (RTGS) network or regional payment interoperability, ensuring the remittance sector can plug into faster, more efficient payment rails as they emerge.

This vision aligns with the Cook Islands' national development goals for an inclusive economy and the global commitments (e.g., UN SDGs) to lower remittance costs and leverage digital finance for growth. It sets a foundation for a **trusted, efficient remittance sector** that empowers communities, strengthens ties with the diaspora, and integrates the Cook Islands into the global financial ecosystem.

3. Purpose, Objectives and Policy Goals

To transform the Money-Changing and Remittance Businesses Act 2009 into a future-proof “Money Services” statute that explicitly captures and regulates both traditional and digital payment activities.

This revamp will equip the Financial Supervisory Commission (FSC) with the authority and tools needed to oversee electronic-money issuers, payment-system operators, mobile-wallet providers, and online P2P remittance platforms—all currently outside the Act’s narrow Section 2 definitions. By doing so, the Cook Islands will eliminate legal ambiguity, foster competition and innovation in fintech, and ensure robust consumer protection across all payment channels.

Objectives

1. Scope Expansion & Clarity

- **Redefinition of “Money Services”:** Replace the cash-only terms in Section 2 with inclusive language that covers electronic-money issuance, clearing and settlement systems (RTGS, ACH), digital remittance platforms, and interoperable wallets.
- **Technology-Neutral Drafting:** Use principles-based drafting to accommodate future innovations—such as API-based account aggregation and tokenized payment rails—without requiring further legislative amendments.

2. Risk-Based Licensing & Proportionality

- **Tiered Framework:** Establish multiple licence categories (e.g., low-value e-wallet, high-volume remitter, system operator) with capital and fee requirements calibrated to each category’s transaction volume and systemic importance.
- **Fast-Track & Sandbox Options:** Introduce a streamlined authorisation pathway for pilot projects and sandbox participants, with clear exit-criteria and sunset clauses, to encourage safe experimentation.

3. Enhanced Supervisory Powers & Transparency

- **Delegated Rulemaking:** Grant the FSC power to issue binding standards and guidance on technical requirements, liquidity buffers, and cyber-resilience measures.
- **Real-Time Reporting & Audit Rights:** Mandate electronic submission of transaction, liquidity and incident-reporting data; empower the FSC to audit on-chain records and algorithmic control logs.
- **Public Register & Disclosure:** Require publication of licence status, key financial metrics, and material regulatory actions to bolster market discipline.

4. **Consumer Protection & Resilience**

- **Fund Segregation & Insolvency Safeguards:** Ensure customer funds held by digital-service providers are ring-fenced in trust or insolvency-remote vehicles.
- **Digital-Channel Disclosures:** Mandate pre-transaction disclosure of fees, exchange rate margins, and complaint resolution procedures via user interfaces and written terms.
- **Electronic Dispute-Resolution Mechanism:** Establish a low-cost, digital first-mile complaints process, with escalation to the FSC and binding mediation/arbitration as needed.

5. **AML/CFT Alignment & Financial Integrity**

- **E-KYC & Digital Identity:** Incorporate FATF's e-KYC and digital-ID best practices, including risk-based customer due diligence and dynamic profile updating.
- **Automated Screening & Monitoring:** Require continuous sanctions screening, transaction pattern analytics, and real-time alerts for thresholds and suspicious activity.
- **Cross-Border Cooperation:** Embed provisions for mutual assistance with foreign supervisors, data-sharing protocols, and joint investigations.

Policy Goals

- **Boost Financial Inclusion:** Lower barriers to entry for digital-only providers, driving down remittance and payment costs—particularly in remote islands where cash logistics are costly.
- **Enhance Market Integrity:** Strengthen oversight of high-velocity electronic payments to detect fraud, cyber-threats and systemic anomalies before they crystallize into broader risks.
- **Provide Regulatory Certainty:** Offer clear, principles-based rules and transparent licensing criteria that give both incumbents and newcomers confidence in their legal obligations.
- **Maintain International Compliance:** Secure the Cook Islands' standing on key AML/CFT and correspondent-bank metrics by aligning domestic law with FATF, UNCITRAL and IOSCO standards.
- **Foster Economic Resilience:** Future-proof the payments ecosystem against technological disruption, supporting sustainable growth of fintech services and digital commerce across all islands.

4. Guiding Principles

FATF Recommendations on AML/CFT (Recs. 15–16)

By embedding the FATF’s guidance on new technologies and wire transfers, the amendments will require every provider—from a small mobile-wallet operator to a high-volume remitter—to implement risk-based customer due diligence processes that leverage digital ID verification, continuous monitoring of transaction flows, and automated sanctions screening. This approach enables the FSC to focus resources on higher risk actors, while smaller firms benefit from streamlined requirements. More importantly, it reassures correspondent banks that the Cook Islands maintains robust defenses against money-laundering and terrorist-financing risks, preserving critical cross-border payment links. Note, the requirements for small firms can remain as they currently are, to avoid overburdening regulatory requirements.

UNCITRAL Model Law on Electronic Commerce (1996)

The “functional equivalence” principle ensures that any electronic act—whether storing value in a wallet, executing a smart-contract transfer, or issuing e-money—carries the same legal validity as depositing cash in a teller’s drawer or signing paper instructions. Drafting around service outcomes rather than specific technologies means the law will automatically encompass future innovations (for example, token-based remittances over decentralized networks) without constant legislative amendments. This flexibility reduces compliance costs for providers and prevents legislative lag as payment methods evolve.

IOSCO Principles for Financial Market Infrastructures

By calibrating licence categories and prudential standards to systemic importance, the reforms will avoid burdening low-volume, community-focused services with the same governance and capital requirements that a central clearinghouse or real-time settlement system demands. Low-value e-wallet providers will face modest capital buffers and lighter reporting duties, while systemically critical platforms will adopt rigorous operational-risk management, board-level cyber-resilience oversight, and periodic third-party audits. This tiered approach promotes healthy market entry without compromising the safety of large-scale payment channels.

UNCDF “Leave No One Behind in the Digital Era”

Financial inclusion is elevated from a policy goal to a binding obligation: licence holders will be expected to design and price services to reach remote islands, low-income households, and underserved groups—especially women and micro-entrepreneurs. By mandating wallet interoperability with bank accounts and requiring user interfaces in local languages, the Act ensures that digital payment solutions do not reinforce existing divides. This principle transforms the payments ecosystem into a driver of equitable economic participation across all communities.

CPMI-IOSCO Principles for Market Transparency

Transparency fosters trust. Requiring a public register that discloses each licence class, key prudential ratios and enforcement actions puts every provider under the same market spotlight. At the same time, standardized disclosures—presented digitally at the point of

transaction and in contract terms—give end-users clarity on fees, exchange-rate margins and their right to dispute. This two-pronged transparency regime not only deters misconduct but also empowers consumers to make informed choices, strengthening the overall integrity of the payments landscape.

5. Rationale for Replacing the Money-Changing and Remittance Business Act 2009

A comprehensive update to the MCRB Act is essential to address current shortcomings and future-proof the regulatory framework. The rationale for this reform is grounded in clear evidence of problems and opportunities, which can be grouped into key areas:

- **Enabling Digital Financial Services and Inclusion:**
 - *Outdated Scope Limiting Innovation:* The 2009 Act was crafted before the advent of many digital financial services. As a result, fintech solutions like mobile money, online remittance apps, and crypto-asset-based transfers operate in a gray area or not at all. Modernizing the Act will create legal pathways for these solutions, enabling providers to launch new services under proper supervision. This will broaden consumer choice and expand access, particularly benefiting citizens in the Pa Enua (outer islands) who currently rely on costly or informal channels.
 - *Reducing Remittance Costs and Improving Efficiency:* High remittance costs are a persistent challenge – fees to send money to the Pacific average around 9%, which erodes the value of funds sent by overseas families. By fostering competition (through more licensed entrants) and new digital delivery channels, the reform aims to drive down costs toward the global target of 3%. More efficient digital processes (e.g., instant mobile transfers instead of cash agent networks) can also shorten transaction times from days to minutes, delivering faster support to households.
- **Strengthening Legal Certainty, Security, and Consumer Trust:**
 - *Regulatory Gaps and Ambiguities:* Under the current law, there is ambiguity in how novel services are treated – for example, are prepaid card issuers or online forex platforms required to be licensed? The absence of clear definitions and categories creates uncertainty that discourages investment and complicates enforcement. The amendments will explicitly define new business categories (such as “**electronic money issuer**” or “**payment service provider**”) and mandate their licensing. Clearer rules will provide legal certainty to providers and consumers alike that these services have the **same legal validity and obligations** as traditional remittance channels.
 - *Improving Consumer Protection:* The existing Act has limited provisions on consumer rights. Complaints handling, refund rights, and liability for fraud or errors are not comprehensively addressed. This can undermine trust—

customers may hesitate to use new services if they fear losing money without recourse. The reform will introduce measures like **mandatory disclosure of fees and exchange rates**, requirements for safeguarding client funds (e.g., segregation of customer monies for remittance companies), and establishing a formal complaint resolution process. Strengthening these protections will boost public confidence in using regulated remittance services over unregulated informal channels.

- *Enhanced Security and Fraud Prevention:* With digital services comes the risk of cyber-fraud and scams. The rationale for reform includes empowering regulators to set **security standards** (for IT systems, data protection, and cybersecurity) for licensed operators. By doing so, the policy ensures that as services go online, adequate safeguards (such as authentication of transactions, encryption of data, and incident reporting duties) are in place to protect users and the financial system.

- **Modernizing the Regulatory and Institutional Framework:**

- *Aligning with Technological Change:* Financial technology is evolving rapidly – from blockchain-based remittances to AI-driven compliance tools – and the law must keep pace. The reform will embed **future-oriented provisions**, such as enabling regulations for electronic KYC (leveraging digital IDs when available) and recognizing electronic records or signatures in compliance processes (in coordination with the ETA). It will also remove any outdated requirements (e.g., paper documentation or physical presence for certain transactions) that no longer make sense in an e-commerce age. This modernization ensures the regulatory environment remains **agile and relevant**, encouraging ongoing digital transformation in the financial sector.
- *Institutional Clarity and Capacity:* Currently, regulatory responsibilities can be fragmented – for instance, the Financial Supervisory Commission oversees licensing and compliance, while the Financial Intelligence Unit handles AML reporting, and the Ministry of Finance sets policy. The rationale for reform includes clarifying roles and coordination mechanisms among these bodies. Amendments may grant the FSC expanded powers to oversee new services and enforce compliance more effectively. Additionally, the reform underscores the need for capacity building: training regulators and law enforcement in supervising digital transactions and investing in modern supervisory tools (like transaction monitoring systems). This will ensure that institutions are **equipped to implement the law**, not just that the law exists on paper.
- *Infrastructure and Ecosystem Readiness:* The Cook Islands currently lacks a real-time national payments infrastructure, and many digital public services are nascent. By updating the MCRB Act now, the country lays the legal groundwork for integrating with or developing such infrastructure. For example, once a national payment switch or RTGS system comes online in the future, licensed remittance providers could be authorized participants, facilitating instant transfers. The reform also complements parallel initiatives

like exploring a Central Bank Digital Currency (if undertaken) or joining regional payment interoperability schemes. In short, it prepares the **ecosystem to adopt new technology** as it becomes available.

In summary, the rationale for reforming the MCRB Act is driven by both **problem gaps** (unregulated services, high costs, consumer risks) and **strategic opportunities** (fintech innovation, regional integration, improved compliance). Updating the law will remove existing impediments to digital finance, bolster the safety and integrity of money transfer channels, and align Cook Islands' practices with international standards and the evolving global landscape of remittances and payments. These changes are crucial for fostering a remittance sector that not only serves the economic needs of today but is resilient and adaptable for tomorrow.

6. National Policy Instruments

- **Legal and Regulatory Instruments**
 - **Amendment Legislation:** Draft a new legal framework to replace the 2009 Act to update definitions, update licensing criteria, and enhance enforcement and electronic-audit powers. Ensure seamless integration with related statutes (Data Privacy, Cybercrime, Consumer Protection) via the Parliamentary Counsel's Office.
 - **Regulations & Guidelines:** Empower the FSC, in consultation with Crown Law and the Ministry of Finance, to issue subordinate regulations covering tiered capital requirements, risk-based licensing procedures, e-KYC protocols, cybersecurity standards, agent-network controls, and dispute resolution processes—allowing technical details to evolve without further primary law amendments.
- **Institutional and Capacity-Building Instruments**
 - **Strengthening Supervisory Bodies:** Establish a dedicated Payments Oversight Unit within the FSC and formalize an MoU with the Financial Intelligence Unit for joint AML/CFT inspections, information sharing, and transaction-monitoring oversight. Train staff on e-money supervision, algorithmic audits, and digital-forensics.
 - **Inter-Agency Coordination:** Create a cross-agency working group—including the Ministry of Finance, Crown Law, FSC, FIU and Telecommunications Regulator—to harmonize oversight of telecom-based wallet operators, manage policy rollout, and resolve jurisdictional overlaps.
- **Guidelines, Standards and Technical Measures**
 - **Digital Compliance Standards:** Develop technical frameworks for e-KYC and digital-ID verification (e.g., biometric and electronic document acceptance) in line with FATF digital-identity guidance.

- **Operational Best Practices:** Issue codes of practice for agent-network management, customer-fund safeguarding in trust accounts or insolvency-remote vehicles, real-time reporting APIs, algorithmic-control audits and incident-reporting protocols.
- **Stakeholder Engagement and Outreach Instruments**
 - **Public-Private Consultations:** Convene ongoing workshops and roundtables with banks, MTOs, fintech startups, community groups and regional partners to co-design regulations, gather real-world feedback, and secure broad buy-in.
 - **Consumer Awareness Campaigns:** Roll out a Digital Payments Awareness Campaign—through community radio, social media and island-council events—highlighting the safety, cost savings and recourse mechanisms of licensed e-channels to build trust and drive adoption.
 - **Industry Capacity Building:** Partner with industry associations and development agencies to deliver certified training for providers on new compliance obligations, cybersecurity risk management and affordable product design.
- **Financial and Incentive Instruments**
 - **Innovation Incentives:** Launch a FinTech Innovation Fund—supported by government and donor grants—to subsidize sandbox participation, capital buffers for low-value e-wallets and pilot projects (e.g., blockchain-based remittance solutions) under FSC oversight.
 - **Fee Structures & Penalties:** Implement a tiered licensing-fee schedule with reduced charges for entities serving outer islands or marginalized groups and enforce graduated sanctions for unlicensed operations or serious compliance breaches to incentivize proper licensure and adherence to standards.
- **Monitoring, Evaluation and Continuous Improvement Instruments**
 - **Regulatory Impact Analysis (RIA):** Track metrics such as remittance costs, number of licensed providers, digital-transaction volumes and compliance incidents on an annual basis to assess whether policy goals—like cost reduction and inclusion—are being met.
 - **Scheduled Review Mechanism:** Mandate a comprehensive review of the Act and related regulations three years post-implementation, incorporating external expert input and new global developments (e.g., CBDCs, updated AML standards) to ensure ongoing relevance and effectiveness.

7. Legislative Harmonization Framework

Money-Changing & Remittance Businesses Act 2009 (Current Framework)

The existing Act regulates currency exchange and inward/outward remittance through two licence classes and basic conduct requirements. It predates digital services and modern AML standards, providing limited enforcement and no coverage for e-money issuers or payment systems. The Amendment Bill will update Section 2 definitions, expand licensing criteria, and introduce new Parts on consumer protection and technology. Existing 2014 Amendment Regulations will be overhauled in tandem to align subordinate rules with the revised Act.

Financial Sector and Banking Laws

Financial supervision lies with the FSC under its 2003 Act, while deposit-taking banks fall under the Banking Act and related regulations. The MCRB reforms will clarify that non-bank money service providers require MCRB licensing—even if they offer remittance via bank channels—and include cross-references to any future National Payment System Act to avoid double licensing and ensure compatibility with systemic payment infrastructure rules.

AML/CFT and Proceeds of Crime Legislation

The Cook Islands' AML/CFT regime (Financial Transactions Reporting Act and regulations) mandates customer-due-diligence and reporting for financial intermediaries. The new Act will explicitly require all licensees to comply with these laws, making non-compliance grounds for licence revocation or penalties. Terms such as “money transfer service” will mirror FATF language to close loopholes and ensure informal remittance channels fall under the same oversight.

Consumer Protection and Competition Laws

General statutes (Fair Trading Act 2008, Consumer Guarantees Act 2008) do not address digital-financial-services specific risks. The MCRB amendments will introduce transparency requirements for fees and exchange rates, dispute-resolution mechanisms, and client-fund safeguards that dovetail with existing definitions of “consumer” and “trade.” Coordination with competition-policy authorities will guard against monopolistic barriers, ensuring that licence requirements do not stifle market entry.

Digital Economy and Electronic Transactions Laws

In anticipation of the forthcoming Electronic Transactions Act, the MCRB amendments employ technology-neutral drafting—avoiding paper-only requirements and enabling online submissions, electronic record-keeping, and digital signatures under the ETA's functional-equivalence provisions. Cross-references and consistent language ensure that once the ETA

is in force, all “written” or “signed” requirements in the MCRB Act automatically include electronic forms.

Emerging Areas and International Obligations

To prepare for an imminent Data Protection Act, basic data-privacy duties are built into the MCRB framework, pending more detailed privacy legislation. Cybersecurity obligations reference anticipated critical infrastructure requirements under the upcoming Cybersecurity Bill, aligning incident-reporting protocols with national response mechanisms. Provisions for cross-border information-sharing and cooperation with foreign regulators reinforce the Cook Islands’ commitments under APG mutual evaluations and UN SDG targets on remittance cost reduction.

Alignment with National Strategies and Initiatives

The harmonization effort supports the Cook Islands National Financial Inclusion Strategy and the Digital Transformation Strategy by embedding inclusion and affordability objectives into licence conditions and incentive schemes. Technical assistance from UNCDF’s Pacific Digital Economy Programme has informed the reforms, ensuring they complement regional best practices and existing policy initiatives rather than proceeding in isolation.

8. Key Stakeholders

Government Agencies

Will provide leadership, regulatory oversight, and the policy coordination needed to develop, implement, and monitor the reformed MCRB framework.

- **Ministry of Finance and Economic Management (MFEM):** Leads policy oversight, aligns reforms with national economic strategies, shepherds the Amendment Bill through Cabinet and Parliament, and monitors macroeconomic impacts.
- **Financial Supervisory Commission (FSC):** Administers licensing, supervision (including AML/CFT), enforcement and public outreach; establishes a Payments Oversight Unit, issues guidelines, conducts inspections/audits, maintains a public register, and chairs stakeholder forums.
- **Crown Law Office & Parliamentary Counsel’s Office:** Drafts amendment legislation and subordinate regulations, ensures drafting consistency, advises on interpretation, and supports enforcement actions.
- **Financial Intelligence Unit (FIU):** Receives and analyzes suspicious transaction reports, collaborates with the FSC under an MoU on e-KYC and transaction-monitoring systems, and coordinates cross-border AML/CFT efforts.

- **Telecommunications and ICT Authority:** Oversees mobile-wallet providers, enforces SIM-registration and network-resilience rules, and ensures real-time reporting capabilities across outer islands.
- **Other Ministries (e.g., Foreign Affairs, Internal Affairs):** Leverage consular networks for diaspora outreach, integrate remittance improvements with social programs, and support community-level adoption.

Private Sector

Will drive innovation and service delivery under the new rules, ensuring compliance while expanding affordable, secure remittance and payment solutions.

- **Money Transfer Operators & Currency Exchange Businesses:** Adapt systems to meet new licensing, AML/CFT and consumer-protection standards; participate in sandbox pilots; educate customers; and form industry associations to share best practices.
- **Banks & Financial Institutions:** Maintain correspondent-banking relationships, provide settlement services and accounts to non-bank providers, and integrate remittance flows into any future National Payment System.
- **Telecommunications & Fintech Companies:** Develop and maintain mobile-money platforms, ensure data security, comply with regulations, and drive adoption through existing subscriber bases and user-education initiatives.
- **Technology Vendors & Agents:** Deliver compliant software solutions (KYC utilities, blockchain remittance engines) and operate as community-based cash-in/cash-out points under agent-oversight guidelines.

Civil Society & Community Organizations

Will advocate for consumer interests, raise awareness, and relay grassroots feedback to ensure the reforms meet end-user needs.

- **Consumer Protection Advocates:** Monitor market practices, gather end-user feedback on fees and disclosures, and partner on financial-literacy workshops and educational materials.
- **Community & Diaspora Groups:** Champion informal-to-formal channel migration, host local demonstration sessions, relay rural and diaspora needs to policymakers, and negotiate better service terms for their communities.
- **Educational Institutions:** Integrate digital-finance curricula, conduct impact research, and pilot emerging technologies in partnership with government and development agencies.

Regional & International Partners

Will supply technical assistance, capacity-building resources, and peer-learning opportunities to bolster implementation and align the Cook Islands with global best practices.

- **Development Agencies (UNCDF, ADB, World Bank, IMF):** Provide technical expertise, data-driven insights on remittance costs and trends, capacity-building grants, and peer-learning opportunities.
- **Pacific Regional Bodies (PFTAC, Pacific Islands Forum):** Coordinate harmonized fintech standards, convene reform-focused workshops, and foster regional interoperability.
- **International Regulatory Networks (APG, Global Forum on Remittances):** Offer updates on emerging AML/CFT threats, best practices, and facilitate cross-border cooperation.
- **Correspondent Banks & Donor Governments:** Maintain banking corridors, support cost-reduction initiatives, and underwrite technical-assistance programs to lower remittance fees for the Cook Islands diaspora.

8. Implementation Roadmap

Below is the integrated Implementation Roadmap, combining the detailed quarterly staging with key activities and lead stakeholders in tabular form:

Phase	Key Activities	Responsible Stakeholders
Phase 1: Legislative Enactment & Initial Outreach (Q3–Q4 2025)	<ul style="list-style-type: none">• Enact the Amendment Act: secure Cabinet approval and Parliamentary passage of the MCRB Amendment Act 2025; publicly gazette new law and commencement date• Draft Supporting Regulations: FSC (with Crown Law & MFEM) develops detailed licensing, fee and compliance rules; informal industry consultation on drafts• Stakeholder Notification: issue circular to existing licensees, conduct media briefings, and host initial outreach sessions	Parliamentary Counsel's Office; Cabinet & Parliament; FSC & Crown Law; Ministry of Finance; Industry Association (if formed); OPM PR Unit

Phase 2: Capacity Building & Transition (Q1–Q2 2026)	<ul style="list-style-type: none"> • Regulator Training: workshops for FSC inspectors, FIU analysts and supporting agencies (with PFTAC/IMF/NZ regulators) on e-money, e-KYC and AML tools • License Transition: re-application period for existing licensees under new criteria; review and issue licences (including fintech entrants) • Industry Guidance & Tools: publish compliance guidelines, deploy online application and reporting portals, host provider clinics • Public Awareness Kick-off: launch consumer campaign (local media, diaspora channels) 	FSC; FIU; Development Partners (UNCDF, etc.); Private Sector; Ministry of Finance / OPM PR Unit; Community Organisations
Phase 3: System Integration & Pilot Programs (Q3 2026–Q2 2027)	<ul style="list-style-type: none"> • Infrastructure Alignment: coordinate with Telecom Authority, banks and regional payments hubs to enable ISO 20022 and sandbox connectivity • Pilot Innovative Services: onboard and supervise sandbox pilots (e.g. mobile wallets in Rarotonga/Aitutaki, low-cost NZ corridor) • Continuous Engagement: quarterly roundtables to resolve teething issues and share success stories • Monitoring Systems: require quarterly data submissions on volumes, fees and complaints; integrate remittance data into FIU analytics 	FSC IT Unit; Telecom Authority; Banks & MNOs; Selected Providers; FSC & Ministry of Finance; Consumer Groups; FIU

Phase 4: Enforcement & Enhancement (Late 2027–2028)	<ul style="list-style-type: none"> • Full Enforcement: end grace periods, conduct inspections (mystery shopping, AML audits), impose sanctions or license revocations for non-compliance • Consumer Protection: analyze complaint patterns, refine guidelines, and operationalize ombudsman/mediation where needed • Interagency Reviews: annual risk meetings (FSC, FIU, Police, Telecom) to address new threats (e.g. crypto remittances) • Legislative Fine-tuning: adjust minor regulatory gaps via FSC directives or prepare future amendments 	FSC Enforcement Division; Police & FIU; Consumer Affairs Office; All Regulators; Crown Law
Phase 5: Evaluation, Scaling & Ongoing Innovation (2029+)	<ul style="list-style-type: none"> • Impact Evaluation: comprehensive study of remittance cost changes, provider and user metrics, and compliance outcomes; publish findings • Policy Adjustments: Cabinet considers action plan for any gaps, new targets, or integration into broader financial-inclusion strategies • Regional Leadership: share lessons in Pacific forums, spearhead regional sandbox initiatives and joint remittance-cost negotiations • Continuous Capacity & Innovation: institutionalize training programs, update sandbox parameters for emerging tech (CBDCs, open APIs) 	Ministry of Finance & FSC; National Statistics Office; UNCDF/Development Partners; Cabinet; Regional Bodies; FSC Innovation Office

Additional Notes

- **Governance & Oversight:** Establish a high-level steering committee—chaired by MFEM and including FSC, FIU and Crown Law—to monitor progress, resolve escalated issues, and authorize any in-flight adjustments to the roadmap.
- **Resource Planning:** Secure dedicated budget lines and staffing for the Payments Oversight Unit, ICT upgrades, training programs and the FinTech Innovation Fund

before Phase 2 begins, to avoid delays in licence reissuance and system deployment.

- **Change Management & Communications:** Develop a comprehensive change-management plan that includes FAQs, user-friendly guidance materials, and a helpdesk function for both industry and consumers. Leverage existing community networks and diaspora channels to reinforce messaging.
- **Risk Mitigation:** Identify “critical path” dependencies (e.g., ICT integration with telecom networks, timely passage of the Amendment Act) and maintain contingency buffers—such as parallel drafting tracks or alternative data-collection methods—to absorb schedule slips.
- **Monitoring & KPIs:** Define a concise dashboard of leading and lagging indicators (e.g., licence-reapplication rates, sandbox uptake, average remittance fee, number of AML/CFT breaches reported) and commit to monthly reviews during Phases 2–4 to surface early warning signs.
- **Feedback Loops:** Embed “rapid-response” clinics during Phases 2 and 3—short, focused working sessions where regulators and providers troubleshoot implementation pain points in real time, minimizing the need for formal regulatory amendments.
- **Legal Continuity:** Maintain a “living” version of the draft Amendment Bill and regulations in a shared repository, so that as policy clarifications arise, they can be captured immediately—ensuring legislative text remains synchronized with operational realities.
- **Sustainability & Handover:** From the outset, plan for the eventual transition of project-team responsibilities into routine FSC workflows, including mentorship, documentation of procedures, and knowledge transfer sessions during Phase 8.

These measures will complement the phased roadmap, ensuring that legislative reform translates into a resilient, well-functioning remittance ecosystem in the Cook Islands.

9. Risks and Mitigation Strategies

1. Legislative Delays

Risk: Protracted Cabinet or Parliamentary debate may postpone enactment, compressing downstream implementation phases.

Mitigation: Maintain early and ongoing engagement with Cabinet ministers and parliamentary committees; prepare concise briefing materials and “question-and-answer” packs; schedule backups for critical milestones (e.g., parallel drafting of regulations).

2. Regulatory Capacity Constraints

Risk: FSC and FIU may lack sufficient skilled staff or technical tools to supervise e-money issuers, real-time reporting, and algorithmic audits.

Mitigation: Front-load recruitment and training in Phase 2; secure donor-funded technical advisors; procure modular transaction-monitoring and e-KYC software before licence reissuance.

3. Industry Resistance or Slow Uptake

Risk: Existing MTOs and new entrants may resist new requirements—particularly sandbox fees, capital buffers, or digital-reporting mandates—leading to non-compliance or minimal participation.

Mitigation: Offer temporary fee waivers or graduated capital thresholds for early adopters; run targeted “implementation clinics” to address provider concerns; publicize pilot successes to incentivize participation.

4. Technology Integration Failures

Risk: Delays or cost overruns in connecting payment-system infrastructure (ISO 20022 messaging, real-time APIs) could stall live operations and data flows.

Mitigation: Adopt a phased technical rollout—starting with non-critical test environments—while securing memoranda of understanding with telecom and banking partners; allocate contingency budget for unforeseen integration work.

5. Consumer Confusion or Distrust

Risk: End-users may mistrust digital channels or misunderstand new disclosure requirements, leading to low adoption or complaints.

Mitigation: Launch a comprehensive, multilingual awareness campaign before Phase 3; deploy community “digital ambassadors” in outer islands; create easy-to-use online and paper guides outlining consumer rights and recourse processes.

6. AML/CFT Compliance Gaps

Risk: Inconsistent transaction-reporting or e-KYC practices could expose the jurisdiction to de-risking by correspondent banks or negative findings in APG evaluations.

Mitigation: Implement standardized reporting templates and automated sanctions-screening tools; conduct joint FSC-FIU audit exercises in Phase 4; schedule a mock APG peer review in Phase 3 to identify gaps early.

7. Funding Shortfalls

Risk: Insufficient budget allocation for the Payments Oversight Unit, IT systems, training, or Innovation Fund grants may hamper execution.

Mitigation: Secure multi-year budget commitments in advance; diversify funding by formalizing donor partnerships (UNCDF, ADB, IMF) with signed MOUs; prioritize critical path expenditures in annual budget planning.

8. Legal Fragmentation

Risk: Incoherence between the amended MCRB Act and other laws (ETA, Data Privacy, Cybercrime) could create compliance confusion or loopholes.

Mitigation: Utilize the inter-agency harmonization working group to review all related statutes concurrently; produce a consolidated “MCRB Act Guide” cross-referencing companion laws; plan for a synchronized review of subordinate regulations six months post-enactment.

By proactively addressing these risks through targeted strategies, the Cook Islands can safeguard the reform process—ensuring that the transformed “Money Services” framework delivers on its goals of inclusion, resilience, and integrity.

10. Conclusion

The proposed reforms to the MCRB Act 2009 serve as a critical pillar in advancing the Cook Islands’ broader digital financial inclusion agenda. By providing a clear, modern, and balanced regulatory framework, the policy establishes the legal certainty and trust necessary for the wider adoption of formal remittance channels and fintech innovations across the Cook Islands. These amendments will drive **financial inclusion** by enabling more competition and digital solutions, thereby extending affordable services to remote communities and underserved groups and fostering sustainable economic empowerment.

Moreover, the reform positions the Cook Islands to **align with international standards and regional peers**, enhancing its credibility and resilience in the global financial system. A well-regulated remittance sector, compliant with FATF standards and leveraging best practices from neighbors, helps safeguard the country from illicit finance risks while facilitating smoother cross-border transactions for diaspora families and businesses. It also supports the modernization of the financial sector, laying groundwork for integration with advanced payment systems and digital economies regionally.

To realize these benefits, **Cabinet endorsement and support are sought** to advance the policy’s implementation as outlined. Key next steps include the formal approval of the amendment legislation, allocation of necessary resources for regulatory capacity building (potentially with development partner assistance), and a mandate for continuous multi-agency collaboration. By championing this reform, the Government will signal its commitment to both **protecting consumers** and **embracing innovation** – a dual objective that is the hallmark of a forward-looking financial policy.

In conclusion, updating the MCRB Act is not just a legal exercise, but a strategic move to empower Cook Islanders through more efficient and secure financial services. It will help

lower the cost of sending money home, ensure that those funds arrive safely and swiftly, and encourage the development of new services that can spur entrepreneurship and economic activity. By adopting this policy and its recommendations, the Cook Islands will strengthen its position as a regional leader in prudent yet progressive financial regulation, unlocking new opportunities for inclusive growth and enhancing the welfare of all its people.

11. Glossary

AML/CFT (Anti-Money Laundering/Countering the Financing of Terrorism): A set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income (money laundering) and to stop funds from being used for terrorist activities. In this document, AML/CFT refers to measures that remittance providers must follow to detect and report suspicious activities and verify customers' identities.

Digital Wallet: An electronic application or service (often on a mobile phone) that allows individuals to store, send, and receive monetary value digitally. In the context of remittances, a digital wallet can hold e-money which users top up and then transfer to others domestically or internationally. The reforms would allow such wallets to be licensed and operate in the Cook Islands, subject to regulation.

E-Money (Electronic Money): Monetary value that is stored electronically or magnetically, commonly used for payment transactions. It is issued on receipt of funds and accepted by parties other than the issuer. Examples include balances held in prepaid cards or mobile money accounts. Under the new framework, e-money issuers (like mobile network operators providing a payment service) would be recognized and regulated under the MCRB Act.

FATF (Financial Action Task Force): An inter-governmental body that sets international standards to combat money laundering, terrorist financing, and related threats. FATF Recommendations are the benchmark for AML/CFT regimes worldwide. FATF Recommendation 14, for example, deals with money transfer services and underpins the need for licensing such services.

FinTech (Financial Technology): Innovative application of technology in the design and delivery of financial services. FinTech in remittances can include online platforms, mobile apps, or blockchain-based services that improve the ease and cost of sending money. The policy encourages FinTech participation in the remittance sector, under appropriate safeguards.

Financial Inclusion: The goal of ensuring individuals and businesses have access to useful and affordable financial products and services – including payments and remittances – that meet their needs and are delivered in a responsible and sustainable way. In this document, financial inclusion refers to extending remittance and exchange services to those who are underserved (e.g., people in remote areas or without bank accounts) through digital channels and more providers.

KYC (Know Your Customer): The process by which businesses verify the identity of their clients, typically during account opening and on an ongoing basis. KYC is a fundamental component of AML compliance. It can include checking official ID documents, verifying phone

numbers or addresses, and understanding the customer's source of funds. Enhanced KYC (including e-KYC using digital tools) is promoted in the reforms to ensure remittance providers know their customers and mitigate risks.

Money-Changing Business: A business that engages in the exchange of one currency for another. Traditionally this might be a bureau de change or a bank offering currency exchange. Under the Act, such businesses require a license. The reforms continue to regulate these, and also consider their digital equivalents (e.g., online forex platforms).

Money Remittance Business: A service that transfers funds from one party to another, either domestically or across borders, without necessarily involving a traditional bank account at one or both ends. Examples include Western Union transfers, online remittance companies, or mobile money remittances. These businesses are the primary subject of the MCRB Act and are being more tightly regulated through the amendments for better oversight and consumer protection.

MVTS (Money or Value Transfer Service): A term often used in international standards (including FATF) to describe services that transfer funds or value for others. It encompasses both formal remittance companies and informal methods (like hawala). Under the reformed law, all MVTS operating in the Cook Islands must be licensed and follow regulations, bringing informal operators into the regulated fold.

Prudential Regulation: Regulations intended to ensure the safety and soundness of financial institutions, protecting consumers' money and maintaining stability. For remittance providers, prudential requirements might include maintaining a minimum capital, bonding or trust account for customer funds, and risk management processes. The reforms introduce proportionate prudential measures to ensure even non-bank providers operate with financial discipline.

RTGS (Real-Time Gross Settlement): A high-value payment system where the transfer of funds or securities occurs in real-time and on a gross (individual transaction) basis. If implemented, an RTGS allows instant and final settlement of interbank transfers. Mentioned in this policy as an aspiration, integration with an RTGS or similar system would allow remittances sent to Cook Islands to be processed and credited much faster than batch or manual systems.

Sandbox (Regulatory Sandbox): A controlled framework that allows fintech innovators to conduct live experiments in a controlled environment under a regulator's supervision. In a sandbox, entities can test new products or services with real customers subject to safeguards and temporary relaxations of some regulatory requirements. This policy contemplates using sandboxes to pilot new remittance technologies in the Cook Islands safely.

Stakeholders: Individuals or organizations with an interest or role in the remittance ecosystem. This includes regulators (like FSC and FIU), government bodies, remittance and forex businesses, banks, consumers (senders and receivers of remittances), and international partners. Stakeholder perspectives were considered in formulating the reforms, and their ongoing engagement is critical for implementation.

UNCDF (United Nations Capital Development Fund): A UN agency that provides investment capital and technical support to reduce poverty and support local development,

especially through financial inclusion and economic empowerment programs. UNCDF's Pacific Digital Economy Programme (PDEP) is mentioned as it assists countries like the Cook Islands in policy development for digital finance. They have been a key partner in providing expertise for this reform initiative.