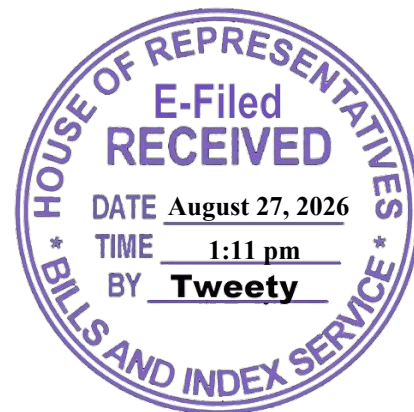


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 11014



Introduced by **HON. MIGUEL LUIS R. VILLAFUERTE, HON. VINCENZO RENATO LUIGI R. VILLAFUERTE, HON. TSUYOSHI ANTHONY G. HORIBATA, AND HON. TERRY L. RIDON**

EXPLANATORY NOTE

Artificial intelligence is rapidly evolving from a technology that merely generates recommendations or content into one capable of acting on behalf of people and businesses. AI agents can increasingly negotiate terms, communicate with counterparties, execute electronic documents, initiate payments, and interact with automated systems without requiring a human to approve every individual step.

Philippine law already recognizes electronic transactions and automated information systems. The next policy challenge is to provide greater legal certainty when increasingly autonomous AI agents perform legally consequential acts: when should an act be attributed to the person who authorized the agent, when may a third party reasonably rely upon that authority, and how should accountability be preserved without granting legal personhood to software?

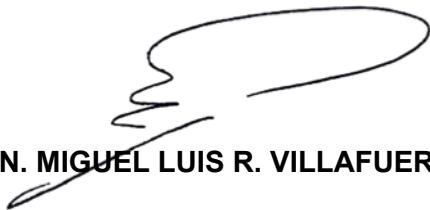
This measure adopts an enabling rather than prohibitory approach. It recognizes AI agents as technological instruments through which natural and juridical persons may act, while ensuring that an identifiable Principal remains accountable. It establishes a primarily voluntary Digital Authority Credential framework so that persons and businesses that need greater certainty may make delegated authority verifiable to counterparties. Mandatory registration is reserved for narrowly designated high-risk autonomous transactions where existing regulation is inadequate.

The measure is also founded on technological neutrality. AI agents may interact with conventional payment systems, application programming interfaces, blockchain networks, smart contracts, digital assets, self-custodial wallets, and future technologies, subject to laws independently applicable to the person or transaction. The Act does not create a new license for digital assets, does not require the registration of wallets or blockchain addresses, does not require disclosure of private keys or seed phrases, and does not prohibit lawful self-custody or peer-to-peer transactions.

The bill likewise protects open-source and non-custodial innovation by providing that developers and infrastructure participants are not treated as Principals or financial intermediaries merely because they publish or maintain software without controlling users' assets or transactions.

The objective is simple: to give Filipinos and Philippine businesses a clear legal framework for using AI agents to transact, while preserving accountability, consumer and third-party protection, privacy, cybersecurity, innovation, competition, and technological freedom.

In view of the foregoing, the immediate passage of this bill is earnestly sought.



HON. MIGUEL LUIS R. VILLAFUERTE



HON. VINCENZO RENATO LUIGI R. VILLAFUERTE



HON. TSUYOSHI ANTHONY G. HORIBATA



HON. TERRY L. RIDON

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 11014

Introduced by **HON. MIGUEL LUIS R. VILLAFUERTE, HON. VINCENZO RENATO LUIGI R. VILLAFUERTE, HON. TSUYOSHI ANTHONY G. HORIBATA, AND HON. TERRY L. RIDON**

AN ACT PROVIDING A LEGAL FRAMEWORK FOR TRANSACTIONS AND OTHER LEGALLY RELEVANT ACTS PERFORMED THROUGH ARTIFICIAL INTELLIGENCE AGENTS, ESTABLISHING A VOLUNTARY DIGITAL AUTHORITY CREDENTIAL FRAMEWORK, PRESERVING ACCOUNTABILITY AND GOOD-FAITH RELIANCE, PROTECTING LAWFUL DIGITAL ASSET OWNERSHIP, SELF-CUSTODY, PEER-TO-PEER AND OPEN-SOURCE TECHNOLOGIES, AND FOR OTHER PURPOSES

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

SECTION 1. Short Title. – This Act shall be known as the "AI Agent Transactions and Accountability Act."

SEC. 2. Declaration of Policy. – The State recognizes the growing use of artificial intelligence agents capable of negotiating, communicating, executing electronic documents, initiating payments, interacting with digital platforms, smart contracts, distributed ledgers, and other systems, and otherwise performing acts capable of producing legal or commercial effects on behalf of natural and juridical persons.

It is the policy of the State to foster the responsible adoption of artificial intelligence and emerging technologies by providing legal certainty as to when acts performed through an Artificial Intelligence Agent are attributable to the person that authorized such Agent.

Towards this end, the State shall:

- (a) recognize the use of Artificial Intelligence Agents as technological instruments through which natural and juridical persons may perform legally relevant electronic acts;
- (b) ensure that the use of an Artificial Intelligence Agent does not create an artificial shield from accountability or confer independent legal personality upon software;
- (c) protect persons who reasonably and in good faith rely upon verifiable manifestations of authority given to an Artificial Intelligence Agent;

- (d) encourage innovation, competition, financial inclusion, and the development and lawful use of artificial intelligence, blockchain, distributed ledger, cryptographic, open-source, and decentralized technologies;
- (e) preserve technological neutrality and avoid imposing regulatory obligations merely because a person chooses one lawful technological architecture over another;
- (f) recognize and protect, subject to existing law, the lawful use of self-hosted and self-custodial digital asset technologies and lawful peer-to-peer transactions; and
- (g) ensure that any registration or credentialing mechanism established under this Act serves primarily as enabling infrastructure for legal certainty and shall not be construed as a general license to develop, deploy, own, or use artificial intelligence or digital assets.

Nothing in this Act shall be construed as granting an Artificial Intelligence Agent natural or juridical personality, constitutional rights, independent ownership rights, or standing to sue or be sued.

SEC. 3. *Definition of Terms.* –

For purposes of this Act:

- (a) "Artificial Intelligence Agent" or "AI Agent" means a software system that uses artificial intelligence to plan, decide, communicate, or execute one or more acts or transactions with limited or no step-by-step human confirmation pursuant to authority granted by a Principal.
- (b) "Principal" means a natural person of legal age or a juridical person recognized under Philippine law that authorizes an AI Agent to act on its behalf.
- (c) "Scope of Authority" means the acts, transactions, limits, conditions, platforms, networks, accounts, wallets, assets, or counterparties in relation to which a Principal has authorized an AI Agent to act.
- (d) "Registered AI Agent" means an AI Agent voluntarily registered under Section 7, or required to be registered pursuant to Section 8, for purposes of obtaining or complying with the verification and reliance mechanisms provided by this Act.
- (e) "Digital Authority Credential" means a cryptographically verifiable or otherwise secure electronic credential through which a third party may verify the identity of the Principal and the relevant Scope of Authority of a Registered AI Agent without requiring disclosure of secret authentication information.
- (f) "Authorized Account or Wallet" means a payment, deposit, securities, digital asset, blockchain, custodial, self-hosted, self-custodial, or other account or wallet over which the Principal has lawful ownership, control, or authority and through which the Principal authorizes an AI Agent to initiate or settle transactions.
- (g) "Self-Custodial Wallet" means a digital asset wallet or technological arrangement through which a person directly controls the cryptographic credentials necessary to authorize transactions without requiring a third-party custodian.
- (h) "Digital Asset" means a digitally represented asset, token, unit of value, or cryptographically secured asset capable of being held or transferred electronically, without prejudice to classifications established under other applicable laws.
- (i) "Transaction Record" means a secure, time-stamped, tamper-evident, or otherwise independently verifiable record sufficient to establish material facts relating to a legally consequential act performed through an AI Agent.
- (j) "Material Excess of Authority" means an act undertaken through an AI Agent that materially exceeds the Scope of Authority granted by the Principal.

SEC. 4. *Legal Recognition and Attribution of Acts Performed Through AI Agents.* – An electronic act, instruction, communication, signature, transaction, or other legally relevant act performed through an AI Agent shall be attributable to the Principal when:

- (a) the act was performed pursuant to the Principal's actual authority;
- (b) the Principal programmed, configured, instructed, authorized, or knowingly permitted the AI Agent to perform acts of that nature; or
- (c) under applicable law, the circumstances otherwise justify attribution to the Principal.

An act attributable to the Principal under this Section shall be treated as an act of the Principal and not as the independent act of the AI Agent.

The use of an AI Agent shall not, by itself, invalidate an electronic contract, electronic signature, payment instruction, or other electronic act that is otherwise valid under Republic Act No. 8792, otherwise known as the Electronic Commerce Act of 2000, the Civil Code, or other applicable law.

Nothing in this Section shall confer independent contractual capacity or legal personality upon an AI Agent.

SEC. 5. *Transactions Through AI Agents.* – Subject to the authority granted by the Principal and applicable law, an AI Agent may be used to:

- (a) negotiate or communicate proposed terms;
- (b) execute electronic signatures, contracts, instructions, and documents attributable to the Principal;
- (c) initiate, authorize, or settle transactions using an Authorized Account or Wallet;
- (d) interact with application programming interfaces, automated systems, smart contracts, distributed ledgers, blockchain networks, and other technological systems; and
- (e) perform other electronic acts capable of producing legal or commercial effects.

Nothing in this Act shall require a human to separately confirm each individual step or transaction where the Principal has lawfully granted the AI Agent authority to act without such step-by-step confirmation.

SEC. 6. *Principal Accountability.* – A Principal shall remain accountable for acts properly attributable to the Principal under Section 4 and may not avoid such accountability solely by asserting that the AI Agent acted autonomously, probabilistically, or without step-by-step human instruction.

Nothing in this Act shall prevent a Principal from proving that a disputed act was not attributable to the Principal because it resulted from:

- (a) theft, forgery, or compromise of credentials;
- (b) unauthorized access or a cybersecurity attack;
- (c) unauthorized material modification of the AI Agent;
- (d) fraud or malicious interference by a third party;
- (e) a material failure of a provider, developer, custodian, platform, or other person outside the Principal's reasonable control; or
- (f) another circumstance recognized under applicable law as negating authority or attribution.

Nothing herein shall prevent contractual indemnification or allocation of liability among Principals, developers, providers, platforms, custodians, and other persons, provided that such arrangements shall not prejudice rights granted to third parties under law.

SEC. 7. *Voluntary AI Agent Registration and Digital Authority Credentials.* – The Department of Information and Communications Technology (DICT) shall establish a

voluntary registration and Digital Authority Credential framework for Principals who wish to provide third parties with a government-recognized means of verifying the delegated authority of an AI Agent.

Registration under this Section shall not be a prerequisite to the lawful development, deployment, possession, or use of an AI Agent, except as expressly provided in Section 8.

The framework shall permit a Principal to register:

- (a) the identity of the Principal;
- (b) sufficient information to identify the AI Agent or class of AI Agents;
- (c) the Scope of Authority;
- (d) relevant transaction limits or conditions, if any; and
- (e) such other information as is reasonably necessary to enable verification of authority.

The DICT shall provide a secure means for a third party to verify whether a Digital Authority Credential is valid, suspended, revoked, or expired and whether the contemplated transaction falls within the relevant registered Scope of Authority.

The framework shall be technologically neutral and shall, to the greatest extent practicable, support interoperable, machine-readable, privacy-preserving, and cryptographically verifiable credentials.

SEC. 8. *Limited Mandatory Registration for High-Risk Autonomous Transactions.* – Registration shall not be mandatory except for specifically designated categories of AI Agents that autonomously undertake high-value, high-risk, or systemically significant transactions and for which existing sectoral regulation does not provide an adequate equivalent mechanism for identity, authority, and accountability.

Any category subject to mandatory registration shall be designated by the DICT only through rules promulgated in coordination with the appropriate sectoral regulator, after public consultation.

In determining whether mandatory registration is necessary, the regulators shall consider:

- (a) transaction value and volume;
- (b) degree of autonomous authority;
- (c) potential financial, safety, or legal harm to third parties;
- (d) systemic or sectoral risk;
- (e) sensitivity of the assets or information involved;
- (f) whether an existing regulatory framework already addresses substantially the same risk; and
- (g) the burden that registration would impose on innovation, competition, small enterprises, and individual users.

No AI Agent shall be subjected to mandatory registration solely because it interacts with a blockchain, distributed ledger, smart contract, Digital Asset, Self-Custodial Wallet, or open-source protocol.

For AI Agents subject to mandatory registration under this Section, the Principal shall comply with additional safeguards proportionate to the nature and risk of the autonomous transactions, which may include technical and security assessment, transaction logging and recordkeeping, human oversight, reasonable means to review, override, or halt transactions

where technically feasible, and other appropriate measures prescribed in the implementing rules and regulations.

SEC. 9. Good-Faith Reliance on Registered Authority. – A person who reasonably and in good faith relies upon a valid Digital Authority Credential and a registered Scope of Authority may rely upon the authority represented therein, subject to applicable law.

Where an AI Agent materially exceeds its registered Scope of Authority:

- (a) a person who knew or reasonably should have known of the lack of authority shall not be entitled to bind the Principal unless the Principal subsequently ratifies the act;
- (b) a person who reasonably and in good faith relied upon a valid Digital Authority Credential shall be protected in accordance with applicable principles of agency, apparent authority, electronic transactions, and other applicable law; and
- (c) the Principal shall retain any right of action or indemnification against any developer, provider, operator, malicious actor, or other responsible person whose breach, negligence, fraud, cybersecurity failure, or wrongful conduct caused or contributed to the excess of authority.

The DICT shall establish procedures for the prompt suspension, revocation, and verification of compromised or superseded Digital Authority Credentials.

SEC. 10. Transaction Records and Auditability. – A Registered AI Agent undertaking legally consequential autonomous transactions shall generate or permit the generation of Transaction Records proportionate to the nature and risk of the activity. Such records shall be securely retained, tamper-evident or otherwise independently verifiable, and sufficient to establish material facts concerning authorization and the transaction.

A public blockchain record, cryptographic proof, digital signature, distributed-ledger record, or equivalent verifiable technological record may satisfy all or part of a recordkeeping or audit requirement under this Act where it reliably establishes the required information.

The DICT and appropriate sectoral regulators may prescribe proportionate retention requirements. No regulation under this Section shall require the creation or centralized retention of information that is unnecessary to establish attribution, authority, or compliance.

SEC. 11. Protection of Digital Asset Ownership, Self-Custody, and Peer-to-Peer Technology. – Nothing in this Act shall be construed to:

- (a) prohibit or restrict the lawful ownership, possession, acquisition, transfer, or use of Digital Assets;
- (b) prohibit or restrict the use of Self-Custodial Wallets or other technologies through which a person directly controls the person's own assets;
- (c) require a person to use a bank, exchange, virtual asset service provider, crypto asset service provider, custodian, or other intermediary solely because an AI Agent interacts with a Digital Asset;
- (d) require the registration, licensing, or government approval of a Digital Asset, blockchain address, wallet, private key, smart contract, decentralized protocol, distributed ledger, or open-source software merely because an AI Agent interacts with such technology;
- (e) require disclosure to the DICT or any registry established under this Act of private keys, seed phrases, passwords, or equivalent secret cryptographic credentials;
- (f) prohibit lawful peer-to-peer transactions conducted without a financial intermediary;

- (g) impose an obligation upon a person solely for developing, publishing, maintaining, validating, or providing open-source, decentralized, or non-custodial software where such person does not exercise control over the user's assets or transactions; or
- (h) expand the jurisdiction of the Bangko Sentral ng Pilipinas (BSP), Securities and Exchange Commission (SEC), Anti-Money Laundering Council (AMLC), DICT, or any other agency beyond that granted under existing law.

Registration of an AI Agent or issuance of a Digital Authority Credential pertains only to the authority delegated by the Principal. It shall not constitute registration, licensing, approval, endorsement, or certification of the underlying Digital Asset, wallet, blockchain, smart contract, protocol, or technology.

Nothing in this Section shall exempt any person or transaction from obligations independently applicable under existing law.

SEC. 12. *Protection of Cryptographic Secrets and Financial Privacy.* – No person shall be required under this Act to surrender or disclose a private key, seed phrase, password, or equivalent secret cryptographic credential as a condition for registration, verification, or lawful use of an AI Agent.

The publicly accessible portion of any registry or verification system established under this Act shall disclose only information reasonably necessary to verify identity, credential status, and relevant authority.

Wallet balances, complete transaction histories, private wallet addresses not necessary for verification, trade secrets, proprietary technical information, and other sensitive financial or cybersecurity information shall not be publicly disclosed under this Act except where disclosure is otherwise required by law or lawful court order.

SEC. 13. *Protection of Developers, Open-Source Software, and Decentralized Protocols.* – A developer, publisher, contributor, validator, node operator, protocol participant, infrastructure provider, or provider of open-source or non-custodial software shall not be deemed the Principal of an AI Agent, a financial intermediary, or a custodian solely by reason of developing, publishing, maintaining, validating, hosting, transmitting, or making software or a protocol available, where such person does not exercise the relevant control over the AI Agent, user assets, or the transaction at issue.

Nothing in this Section shall exempt a person from liability arising from that person's own fraud, intentional misconduct, contractual undertaking, or other liability independently established under applicable law.

SEC. 14. *Responsible Configuration and Conflicts of Interest.* – A Principal and, where applicable, a provider responsible for configuring or operating a Registered AI Agent shall take reasonable and proportionate measures to ensure that the AI Agent operates consistently with the authority granted to it.

A provider shall disclose to the Principal any material arrangement known to the provider, including referral fees, preferential routing, commissions, or revenue-sharing arrangements, that could reasonably influence the AI Agent's recommendations or transactions in a manner contrary to the Principal's stated instructions or interests.

SEC. 15. *Risk-Based Financial Security.* – The DICT, in coordination with the appropriate sectoral regulator, may require insurance, a bond, reserve, or other reasonable financial security only for categories of Registered AI Agents presenting a substantial risk of financial harm to third parties.

Any such requirement shall be proportionate to transaction volume, maximum transaction value, nature of assets involved, degree of autonomous authority, existing safeguards, and potential third-party harm.

Low-risk and low-value AI Agents shall be exempt from such requirement unless otherwise required under an independently applicable law or sectoral regulation.

SEC. 16. *Suspension and Revocation of Digital Authority Credentials.* – The DICT may, after due notice and opportunity to be heard, suspend or revoke a Digital Authority Credential for material misrepresentation, repeated material excesses of registered authority resulting from inadequate safeguards, knowing misuse of the credential, or material failure to comply with requirements applicable to Registered AI Agents under this Act.

The DICT may temporarily suspend a credential without prior hearing where reasonably necessary to prevent imminent fraud, theft, cybersecurity harm, or substantial injury, provided that the Principal shall be afforded prompt post-suspension review.

A Principal may revoke or terminate a voluntary registration or credential at any time, without prejudice to obligations arising from transactions validly initiated before such revocation or termination became effective and reasonably discoverable by third parties.

SEC. 17. *Prohibited Acts and Penalties.* – It shall be unlawful for any person to:

- (a) knowingly and materially falsify information in an application for a Digital Authority Credential;
- (b) falsify, forge, steal, or knowingly misuse a Digital Authority Credential;
- (c) knowingly operate an AI Agent without registration where registration has been expressly and validly required under Section 8;
- (d) knowingly use a Registered AI Agent or Digital Authority Credential to commit fraud or deliberately circumvent a law independently applicable to the person or transaction; or
- (e) fraudulently represent registration as conferring legal personality upon an AI Agent or as constituting government endorsement of an AI Agent, Digital Asset, wallet, blockchain, protocol, or commercial product.

Minor registration, reporting, or recordkeeping violations shall be subject to proportionate administrative sanctions.

Criminal penalties shall apply only to knowing or willful conduct involving fraud, intentional falsification, deliberate circumvention of applicable law, theft or misuse of credentials, or comparable serious misconduct.

Any person who knowingly or willfully commits an offense under paragraphs (a), (b), or (d) involving fraud or deliberate circumvention of law shall be punished by a fine of not less than Two Hundred Thousand Pesos (P200,000.00) but not more than Two Million Pesos (P2,000,000.00), or imprisonment of not less than six (6) months but not more than six (6) years, or both, at the discretion of the court, without prejudice to liability under other applicable laws.

SEC. 18. *Relationship with Existing Financial, Digital Asset, and Sectoral Regulation.* – Nothing in this Act shall be construed to expand, diminish, or alter the jurisdiction granted by existing law to the BSP, SEC, AMLC, NPC, or other sectoral regulators.

Customer identification, anti-money laundering, travel rule, licensing, registration, consumer protection, securities, banking, payment system, and other sectoral requirements shall apply only to the extent that they are independently applicable under existing law.

Compliance with this Act shall not, by itself, cause a person who is not otherwise a regulated financial intermediary, virtual asset service provider, crypto asset service provider, custodian, or covered person to become one solely because the person uses or provides an AI Agent.

Where an existing sectoral framework provides a substantially equivalent mechanism for identity, authority, accountability, auditability, or transaction verification, the implementing agencies shall recognize such mechanism to avoid duplicative regulation.

SEC. 19. *Interface with Subsequent Artificial Intelligence Legislation.* – Nothing in this Act shall independently establish a comprehensive system for classifying the general risk level or permissible uses of artificial intelligence.

Upon the effectivity of a subsequent law establishing a dedicated artificial intelligence regulatory authority, functions under this Act may be transferred to such authority only to the extent expressly provided by law.

Any subsequent implementation of this Act shall preserve its principles of technological neutrality, proportionate regulation, legal attribution, protection of lawful self-custody, and avoidance of duplicative regulation unless otherwise expressly provided by Congress.

SEC. 20. *Regulatory Sandbox and Interoperability.* – The DICT, in coordination with appropriate sectoral regulators, may establish a regulatory sandbox or controlled testing environment for voluntary Digital Authority Credentials, machine-to-machine transactions, AI Agent authentication, privacy-preserving verification, and interoperable transaction standards. Participation in such sandbox shall not be construed as a prerequisite to lawful innovation outside the sandbox where the activity is otherwise lawful.

The government shall, where practicable, favor open standards, interoperability, portability, and competition and shall avoid technical requirements that unnecessarily lock users or businesses into a single vendor, platform, custodian, or technological architecture.

SEC. 21. *Mandatory Congressional Review.* – Congress shall review the implementation of this Act three (3) years after its effectivity. The DICT shall submit a report covering:

- (a) adoption of voluntary Digital Authority Credentials;
- (b) categories, volume, and value of transactions using Registered AI Agents, using aggregated information where appropriate;
- (c) disputes involving attribution or excess of authority;
- (d) cybersecurity incidents involving Registered AI Agents;
- (e) enforcement actions;
- (f) impact upon innovation, competition, financial inclusion, small enterprises, and adoption of emerging technologies;
- (g) whether mandatory registration under Section 8 remains necessary for any designated category; and
- (h) whether any provision or implementing rule has unnecessarily restricted self-custody, lawful peer-to-peer activity, open-source development, decentralized technologies, or lawful Digital Asset activity.

The report shall include recommendations for amendment, simplification, deregulation, or repeal of requirements that have become unnecessary or disproportionate.

SEC. 22. Appropriations. – The amount necessary for the initial implementation of this Act shall be charged against the current appropriations of the DICT. Thereafter, such sums as may be necessary shall be included in the annual General Appropriations Act.

SEC. 23. Implementing Rules and Regulations. – Within one hundred twenty (120) days from the effectivity of this Act, the DICT, in coordination with the SEC, BSP, NPC, AMLC, Department of Trade and Industry, and other appropriate agencies, and after public consultation with industry, consumer, technology, open-source, academic, financial, and digital asset stakeholders, shall promulgate the implementing rules and regulations.

The implementing rules shall:

- (a) be technologically neutral;
- (b) employ risk-based and proportionate regulation;
- (c) minimize unnecessary barriers to innovation, competition, and market entry;
- (d) avoid duplicative regulation and recognize substantially equivalent sectoral safeguards;
- (e) preserve cybersecurity, privacy, trade secrets, and commercially sensitive information;
- (f) not require disclosure of private keys, seed phrases, or equivalent cryptographic secrets;
- (g) not expand the jurisdiction of any participating agency beyond that granted by law; and
- (h) provide reasonable compliance pathways for individuals, startups, small and medium enterprises, open-source projects, and other innovators.

SEC. 24. Separability Clause. – If any section or part of this Act is held unconstitutional or invalid, the other sections or provisions not otherwise affected shall remain in full force and effect.

SEC. 25. Repealing Clause. – All laws, decrees, executive orders, rules and regulations, issuances or any part thereof inconsistent with the provisions of this Act, are hereby repealed, amended or modified accordingly.

SEC. 26. Effectivity. – This Act shall take effect fifteen (15) days after its publication in the *Official Gazette* or in at least two (2) national newspapers of general circulation.

Approved,