

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City
TWENTIETH CONGRESS
First Regular Session
House Bill No. 6696



Introduced by Representative
Brian Poe, PhD, MNSA.

AN ACT MANDATING THE VERIFICATION AND AUTHENTICATION OF OFFICIAL AND CORPORATE CALLER IDENTITIES TO PREVENT TELECOMMUNICATIONS FRAUD, CREATING THE NECESSARY REGISTRIES, AND PRESCRIBING PENALTIES FOR VIOLATIONS THEREOF.

EXPLANATORY NOTE

The rapid escalation of digital fraud in the Philippines now presents a significant systemic threat to national economic stability and to consumer trust in electronic communications. While earlier measures—most notably the SIM Registration Act (Republic Act No. 11934)—have successfully reduced text-based fraud by improving mobile number attribution, criminal syndicates have quickly adapted. Their operations have shifted from anonymous messages to highly targeted and institutionally-impersonated voice calls and social media outreach.

This shift has exposed a critical weakness in the country's telecommunications ecosystem. Sophisticated voice-based scams now proliferate, generating staggering economic losses: an estimated USD 8.29 billion (approximately ₱480 billion) annually, or 1.9% of national GDP¹. Within a recent three-month period, 74% of Filipinos² reported being targeted by scammers, and

¹ <https://newsinfo.inquirer.net/1993340/alarming-p460b-lost-to-scams-in-ph-says-study>

²

<https://fintechnews.ph/66774/security/philippines-records-elevated-digital-fraud-rate-for-5th-consecutive-year/>

45%³ of victims suffered emotional distress⁴. These figures underscore the urgent need for legislation that secures institutional identities in the voice channel.⁵

Evidence shows that the success of the SIM Registration Act inadvertently displaced criminal activity toward call-based fraud. In the first quarter of 2025 alone, scam calls surged by 74%, rising from 108,157 to 351,699⁶—equivalent to a 225% year-on-year increase. Most of these attacks involve institutional impersonation. Loan availment scams constitute 55% of fraudulent calls, while collection-related scams account for another 10%. Criminal groups exploit the absence of mandatory Caller ID authentication to mimic banks, government agencies, utilities, and other high-trust entities. Although current regulations penalize caller spoofing, they do not impose a technical, network-level mechanism to prevent it—leaving consumers exposed.

The proposed “Secure Call Act” closes this institutional identity gap. It mandates the registration of official contact numbers, requires Public Telecommunications Entities (PTEs) to adopt global-standard cryptographic call authentication, and establishes a Verified Corporate Caller Identity (VCCI) framework to ensure the public can trust the identity displayed on their device before answering. With victims losing an average of ₱44,700—nearly two months’ wages for many households—this measure is essential not only for consumer protection but also for national financial stability and cybersecurity.

The “Secure Call Act” establishes a unified, verifiable, and enforceable identity framework for government and corporate outbound communications. Its principal objectives are as follows:

1. **Mandatory Identity Registration and Verification**

Require all Government Agencies and designated high-risk corporate entities to register and verify their Official Contact Numbers (OCNs) through dedicated, secure registries.

2. **Technical Authentication Requirements**

Mandate Public Telecommunications Entity (PTE) implementation of Secure Telephony Identity Revisited (STIR)/ Signature-based Handling of Asserted information using toKENs (SHAKEN) and related cryptographic standards to prevent caller ID spoofing and ensure authoritative traceability.

3. **Jurisdictional Clarity and Portal Creation**

Define the regulatory roles of DICT/NTC for technical and government identity oversight and the SEC for corporate identity verification, leveraging existing infrastructure such as eSECURE and SCORE.

4. **Robust Enforcement and Deterrence**

Impose penalties proportionate to the scale of digital fraud, ensuring meaningful compliance and reinforcing related statutes, including the Cybercrime Prevention Act (RA 10175) and SIM Registration Act (RA 11934).

³<https://www.manilatimes.net/2025/11/25/news/national/filipinos-among-most-targeted-consumers-in-asia-by-scammers-report/2231252>

⁴<https://newsroom.transunion.ph/philippines-suspected-digital-fraud-rate-higher-than-global-level-for-fifth-consecutive-year/>

⁵<https://www.gsma.com/newsroom/press-release/rising-scam-exposure-in-the-philippines-underscores-need-for-cross-sector-action-warns-new-gsma-report/>

⁶<https://www.manilatimes.net/2025/04/30/business/top-business/the-alarming-rise-of-fraudulent-calls-in-the-philippines/2101888>

In lieu of the foregoing, we seek the immediate passage of this bill into law.

Approved,

A handwritten signature in black ink, reading "Brian Poe". The signature is fluid and cursive, with a long horizontal stroke extending from the end of the name.

HON. BRIAN POE, PhD, MNSA.

Representative

FPJ Panday Bayanihan Party-List

Republic of the Philippines
HOUSE OF REPRESENTATIVES

Quezon City

TWENTIETH CONGRESS

First Regular Session

House Bill No. 6696

Introduced by Representative

Brian Poe, PhD, MNSA.

AN ACT MANDATING THE VERIFICATION AND AUTHENTICATION OF OFFICIAL AND CORPORATE CALLER IDENTITIES TO PREVENT TELECOMMUNICATIONS FRAUD, CREATING THE NECESSARY REGISTRIES, AND PRESCRIBING PENALTIES FOR VIOLATIONS THEREOF

Article I: General Provisions

Section 1. Short Title. – This Act shall be known as “The Secure Call Act.”

Section 2. Declaration of Policy. – It is hereby declared the policy of the State to ensure the integrity, security, and reliability of the national telecommunications network, recognizing it as a vital tool for nation-building and development. The State shall protect consumers against the misuse of telecommunications services, specifically aiming to prevent the proliferation of financial and identity fraud (cybercrime) perpetuated through unverified voice calls and messages. To this end, the State shall mandate the verification and cryptographic authentication of institutional callers—both governmental and private—to restore public trust in official electronic communications.

Section 3. Definition of Terms. – As used in this Act, the following terms shall mean:

- a) Public Telecommunications Entity (PTE): Any person, firm, partnership, or corporation engaged in the provision of telecommunications services to the public for compensation, as defined in Republic Act No. 7925.
- b) Primary Caller: Any juridical entity, public or private, required under this Act to register its Official Contact Numbers, including but not limited to banks, corporations, government agencies, and public utilities.

c) Official Contact Number (OCN): A specific telephone number, either mobile or landline, designated and registered by a Primary Caller for official outbound communication with the public, customers, or beneficiaries.

d) Verified Corporate Caller Identity (VCCI): The corporate or trade name of a registered Primary Caller, verified against official SEC or DICT records, which is cryptographically authenticated and displayed upon the recipient's telecommunications device, conforming to technical standards for Rich Call Data (RCD) or Calling Name Presentation (CNAP).

e) Call Spoofing: The act of transmitting misleading or inaccurate information about the source of the phone call, with the intent to defraud, cause harm, or wrongfully obtain anything of value.

f) Call Authentication Framework (CAF): The industry-standard technical infrastructure, specifically including Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN), mandated for implementation by PTEs to verify the legitimacy of the OCN.

g) Verified Attestation: The technical indicator provided by the originating PTE (such as A-Level Attestation) confirming that the VCCI is non-spoofed and that the call originator is authorized to use the OCN.

Article II: Mandatory Registration and Verification

Section 4. Government Caller ID Registry (GCIDR). – The Department of Information and Communications Technology (DICT), in coordination with the National Telecommunications Commission (NTC), shall establish, operate, and maintain the Government Caller ID Registry (GCIDR). The GCIDR shall be a centralized, high-security, and publicly accessible database of all Official Contact Numbers (OCNs) used by all National and Local Government Agencies, including Government-Owned and Controlled Corporations (GOCCs). All Government Agencies are mandated to register their OCNs, authorized users, and the documented purpose of the call (e.g., "Tax Notification," "Visa Inquiry"). The GCIDR shall facilitate the issuance of authenticated cryptographic keys to PTEs to enable A-Level Attestation for government-originated calls, utilizing the existing Philippine National Public Key Infrastructure (PNPKI) framework for digital identity assurance. This measure adopts the successful international model of standardizing government identity to effectively neutralize official impersonation scams.

Section 5. Private Sector Verified Caller Identity Portal (VCCIP). – The Securities and Exchange Commission (SEC) is hereby mandated to establish, operate, and maintain the Private Sector Verified Caller Identity Portal (VCCIP). The SEC shall leverage its existing technological infrastructure, including the Electronic SEC User Registration Environment (eSECURE) and the SEC Swift Corporate and Other Records Exchange Protocol (SCORE), which already perform risk-based credentialing, eKYC, and secure corporate document exchange.

- a) Registration: Primary Callers (juridical entities) shall be required to register all OCNs with the SEC, linking each number directly to their official corporate name, General Information Sheet (GIS) records, and industry classification.
- b) Verification: The SEC shall verify the OCN against the identity of the juridical entity, its beneficial owners, and its official regulatory compliance records.
- c) Authentication Authorization: Upon successful verification, the SEC shall authorize the issuance of the necessary digital certificates or tokens required for STIR/SHAKEN signing to the Primary Caller's originating PTE. The VCCIP shall function as the primary repository of corporate identity data used for call authentication, providing the essential corporate identity verification component for the Call Authentication Framework.

Section 6. Designated Primary Industries for Mandatory Registration. – Mandatory registration under the VCCIP shall apply immediately to all juridical entities operating within industries where impersonation and financial fraud pose the highest systemic risk, including, but not limited to, the following:

- a) Financial Sector: All Banks, Quasi-Banks, Non-Bank Financial Institutions, Investment Advisers, E-Money Issuers, and Lending/Financing Companies regulated by the Bangko Sentral ng Pilipinas (BSP) and the SEC. These entities are the primary targets of loan availment and collection scams, which constitute the majority of call-based fraud.
- b) Capital Markets: All Publicly Listed Companies (PLCs) and registered Issuers of Securities.
- c) E-Commerce and Logistics: Major E-Commerce Platforms, Online Retailers, and registered Logistics and Delivery Services, which are frequently mimicked in online shopping and fake delivery fee requests.
- d) Public Utilities: Public Telecommunications Entities (PTEs), and registered providers of electricity, water, and other essential public services.

The SEC, in consultation with the NTC and the relevant industry regulators (such as the BSP and DTI), is authorized to expand this list via the Implementing Rules and Regulations (IRR) to address emerging fraud vectors.

Article III: Technical Implementation and Duties of PTEs

Section 7. Mandate for Call Authentication Framework Implementation. – All Public Telecommunications Entities (PTEs) providing voice services over Internet Protocol (IP) networks shall be required to implement the necessary hardware, software, and Public Key Infrastructure (PKI) required for the Call Authentication Framework (STIR/SHAKEN). This implementation must be completed within eighteen (18) months from the effectivity of this Act, or within a stricter timeframe determined by the NTC based on emerging technological feasibility and national security concerns. The PTEs' capital expenditure for this framework is determined to be a

necessary public interest investment to mitigate the estimated P480 billion annual losses due to fraud.

Furthermore, the NTC shall mandate all PTEs to integrate protocols for Rich Call Data (RCD) or an equivalent Calling Name Presentation (CNAP) technology to ensure the Verified Corporate Caller Identity (VCCI) or Official Contact Number (OCN) name is displayed on the recipient's handset, regardless of the handset's sophistication.

Section 8. Duties Regarding Verified Calls.

The technical integrity of all institutional calls shall be governed by the following duties:

- a) **Originating PTE Duty:** The Originating PTE shall cryptographically sign all outbound calls originating from registered Primary Callers using the appropriate Verified Attestation Level (preferably A-Level Attestation). This signing must utilize the digital certificates authorized by the VCCIP (SEC) or GCIDR (DICT), ensuring the corporate identity is authenticated at the source.
- b) **Terminating PTE Duty:** The Terminating PTE shall verify the digital signature contained within the Call Authentication Framework payload. If an A-Level Attestation is verified, the Terminating PTE shall be required to present the VCCI or OCN name to the subscriber, along with a clear visual verification indicator (e.g., a checkmark or verified tag) on the consumer's handset. This public display provides immediate and verifiable trust to the consumer.

Section 9. Handling of Unverified and Spoofed Calls. – PTEs shall implement network analytics and robust fraud mitigation solutions to monitor and manage calls lacking Verified Attestation. Calls originating from an OCN or VCCI but lacking the proper A-Level digital signature shall be identified as potentially fraudulent. The NTC shall issue guidelines requiring PTEs to deploy mechanisms to detect and block calls identified as spoofed (i.e., those attempting to transmit an OCN/VCCI without the requisite authentication token) and establish guidelines for how calls with only Partial (B) or Gateway (C) Attestation should be labeled and displayed to the consumer to maximize protection.

Article IV: Enforcement, Penalties, and Funding

The enforcement provisions reflect the view that telecommunications fraud is a systemic financial and cybersecurity risk, requiring penalties that serve as effective deterrents to large corporations and PTEs.

Section 10. Penalties for Corporate Non-Compliance (SEC Jurisdiction). – Any Primary Caller who fails to register an OCN within the period prescribed in the IRR, or who knowingly submits false or misleading information to the VCCIP, shall be subject to administrative fines imposed by the SEC, pursuant to its enforcement authority under the Securities Regulation Code and the Revised Corporation Code.

- a) **Fines:** Fines shall range from One Hundred Thousand Pesos (₱100,000.00) up to Two Million Pesos (₱2,000,000.00) per violation.

- b) Corporate Sanctions: Repeat or egregious violations, especially those leading to consumer harm, shall be grounds for the disqualification of responsible directors, trustees, and officers from holding their positions for a period of up to five (5) years, and/or the suspension or revocation of the entity's Certificate of Incorporation. These penalties are deemed necessary to enforce due diligence in corporate identity disclosure and security.

Section 11. Penalties for PTE Non-Compliance (NTC Jurisdiction). – Any Public Telecommunications Entity (PTE) that fails to implement the Call Authentication Framework (STIR/SHAKEN) within the prescribed period, or fails to properly sign or verify calls resulting in consumer harm or unmitigated spoofing, shall be subject to administrative fines imposed by the NTC. The existing administrative fine limits under various laws (e.g., up to ₱300,000) are determined to be grossly inadequate to deter non-compliance given the multi-billion peso cost of fraud exposure. Therefore, the following escalated fine structure is mandated:

- a) Initial Failure to Implement: A fine starting at Five Hundred Thousand Pesos (₱500,000.00) up to Ten Million Pesos (₱10,000,000.00) shall be imposed for initial failures to implement the Call Authentication Framework.
- b) Systemic Failures: For systemic failures or for the fifth and subsequent instances of failure to properly authenticate or mitigate spoofed calls, the NTC shall recommend to the relevant authorizing body the revocation of the PTE's Certificate of Public Convenience and Necessity or franchise to operate.

Section 12. Criminal Penalties for Spoofing. – Intentional Call Spoofing, defined as transmitting misleading VCCI or OCN with intent to defraud or cause harm, shall be punishable under Republic Act No. 11934 (SIM Registration Act), Section 11(e) with imprisonment of no less than six (6) years, or a fine of Two Hundred Thousand Pesos (₱200,000.00), or both. The verification and authentication data collected and stored by the VCCIP and GCIDR shall serve as essential prima facie evidence in all criminal and civil proceedings related to cybercrime and identity fraud.

Section 13. Funding. – Congress shall appropriate the initial necessary funds for the DICT and SEC for the establishment, maintenance, and secure operation of the GCIDR and VCCIP, respectively. The SEC and NTC shall be authorized to impose reasonable, risk-based registration and certificate fees on registered Primary Callers to cover the perpetual operational and certification costs associated with maintaining the authentication infrastructure and registries.

Article V: Final Provisions

Section 14. Implementing Rules and Regulations (IRR). – The DICT, NTC, SEC, and National Privacy Commission (NPC) shall jointly formulate the Implementing Rules and Regulations (IRR) necessary to effectively implement the provisions of this Act within ninety (90) days from its effectivity. This joint mandate is intended to preempt potential regulatory silos and jurisdictional conflicts, ensuring a harmonized policy that addresses technical enforcement (NTC), corporate identity (SEC), government security (DICT), and data privacy compliance (NPC).

Section 15. Separability Clause. – Should any provision of this Act be declared unconstitutional or invalid, the other provisions not affected thereby shall remain valid and effective.

Section 16. Repealing Clause. – All laws, decrees, orders, rules and regulations or parts thereof inconsistent with this Act are hereby repealed or modified accordingly.

Section 17. Effectivity. – This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved,


HON. BRIAN POE, PhD, MNSA.
Representative
FPJ Panday Bayanihan Party-List