

REPUBLIC OF THE PHILIPPINES



House of Representatives
CONSTITUTION HILLS, QUEZON CITY

TWENTIETH CONGRESS
First Regular Session

House Bill No. 6554



**AN ACT STRENGTHENING THE PROTECTION OF SENIOR CITIZENS
AGAINST ONLINE SCAMS, FINANCIAL FRAUD, AND DIGITAL
EXPLOITATION, MANDATING RAPID RESPONSE MECHANISMS, ENHANCING
LEGAL REMEDIES, AND FOR OTHER PURPOSES**

Introduced by Representative SHIRLYN L. BAÑAS-NOGRALES

EXPLANATORY NOTE

Filipino senior citizens, defined under Republic Act No. 9994 as persons aged sixty (60) and above, constitute a population that requires targeted support in the rapidly evolving digital economy. While online banking, e-commerce, and electronic government services have enhanced convenience and accessibility, these platforms also expose older adults to heightened risks of fraud, identity theft, and online exploitation. As digital immigrants – having been born before the widespread adoption of digital technology – seniors face unique challenges in safely navigating these systems.

Reports from the Cybercrime Investigation and Coordinating Center (CICC) and the Philippine National Police – Anti-Cybercrime Group (PNP-ACG) show a significant rise in online fraud, including phishing, fake investment schemes, SIM-swap fraud, bogus medical or pension solicitations, romance scams, and account takeovers (CICC, 2025; Philippine News Agency [PNA], 2025). In 2024, approximately 3,200–3,500 online-fraud complaints were recorded nationwide, with an estimated 288–385 involving senior citizens (CICC, 2025). Seniors' vulnerability is worsened by low digital literacy – only 38% are considered “basic” digital users – and low reporting rates due to stigma, fear, and procedural complexity (DICT, 2024).

Projections indicate that, without intervention, senior-victim complaints could rise to 463–620 cases by 2029. With partial awareness programs, complaints may increase to 368–490 cases. Full implementation of this proposed measure – including senior-focused cyber-fraud desks, mandatory reimbursement protocols, barangay-based Senior Cyber Support Teams (SCSTs), and interoperable digital systems across government agencies and financial institutions – could reduce incidents to 170–228 cases by 2029, representing a potential decrease of nearly half.

Although these figures are estimates due to the absence of age-disaggregated official data, they highlight the urgent need for a legislative framework specifically protecting senior citizens from online exploitation. This proposed law seeks to address these vulnerabilities by enhancing penalties for crimes committed against senior citizens online, mandating a 15-day reimbursement window for elder victims of online financial fraud, establishing Senior Cyber-Fraud Desks in all PNP stations and NBI offices, institutionalizing the Senior Citizen Cyber

Protection Program (SCCPP) to coordinate prevention, reporting, and enforcement across agencies, requiring banks and e-wallet providers to adopt advanced authentication systems that do not rely solely on SMS One-Time Passwords (OTPs), organizing LGU-based SCSTs to provide grassroots digital support, deploying multilingual digital literacy modules tailored for elders, and ensuring rapid data preservation, asset freezing, and inter-agency coordination for restitution. The emphasis on interoperability ensures that government and financial systems work seamlessly together to facilitate timely protection, reporting, and recovery for senior.

Despite the presence of laws such as the Cybercrime Prevention Act (R.A. 10175), the Access Devices Regulation Act (R.A. 8484), the Data Privacy Act (R.A. 10173), the Financial Consumer Protection Act (R.A. 11765), and the SIM Registration Act (R.A. 11934), none of these statutes provide age-specific safeguards for senior citizens. This gap leaves vulnerabilities that online criminals continue to exploit. Persistent enforcement challenges, fragmented reporting mechanisms, limited digital literacy among older adults, the rise of cross-border cyber offenders, and delays in financial restitution have created an environment where online fraud targeting seniors can thrive.

Finally, the State has a moral and Constitutional duty to protect senior citizens from exploitation and abuse – whether physical, financial, or digital. As transactions increasingly migrate online, our laws must evolve to ensure that elders are not left behind, unprotected, or unseen.

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



SHIRLYN L. BAÑAS-NOGRALES



REPUBLIC OF THE PHILIPPINES

House of Representatives

CONSTITUTION HILLS, QUEZON CITY

TWENTIETH CONGRESS

First Regular Session

House Bill No. 6554

AN ACT STRENGTHENING THE PROTECTION OF SENIOR CITIZENS AGAINST ONLINE SCAMS, FINANCIAL FRAUD, AND DIGITAL EXPLOITATION, MANDATING RAPID RESPONSE MECHANISMS, ENHANCING LEGAL REMEDIES, AND FOR OTHER PURPOSES

Introduced by Representative SHIRLYN L. BAÑAS-NOGRALES

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 “*Safe Seniors Online Act of 2025*”.

SECTION 2. Declaration of Policy. – It is the policy of the State, pursuant to Article II, Section 5, Article XIII, Section 11, and Article XV, Section 4 of the 1987 Philippine Constitution, to protect and promote the well-being of Filipino senior citizens. In line with this mandate, the State shall safeguard seniors from online scams, cyber-enabled fraud, and financial exploitation. The State shall also strengthen enforcement mechanisms against emerging digital fraud schemes targeting persons aged sixty (60) years and above, ensure rapid restitution and digital assistance, and provide age-appropriate reporting channels.

Furthermore, the State shall promote digital literacy and cyber-safety among senior citizens, and enhance **inter-agency coordination and interoperability of systems** to prevent, detect, investigate, and prosecute online crimes affecting elder victims. The principle of interoperability shall guide the design and operation of the **Senior Citizen Cyber Protection Program (SCCPP)**, Senior Cyber-Fraud Desks, and LGU-based **Senior Cyber Support Teams (SCSTs)**, ensuring that government agencies, financial institutions, and local units share relevant data, coordinate responses, and provide seamless assistance to senior victims of online exploitation.

3. Definition of Terms. – For purposes of this Act:

- a.) **Senior Citizen/Elder** refers to any person aged sixty (60) years or above as defined under R.A. 9994.
- b.) **Online Scam/Cyber Fraud** refers to any act committed through electronic means that deceives, misappropriates, or defrauds a senior citizen, including but not limited to phishing, identity theft, SIM-swap fraud, fake investment schemes, romance scams, grandparent scams, tech-support scams, account takeovers, and fraudulent solicitations.

- c.) **Financial Service Provider (FSP)** refers to banks, e-money issuers, non-bank financial institutions, and digital platforms regulated by the *Bangko Sentral ng Pilipinas* (BSP).
- d.) **Behavioral Biometrics/Advanced Authentication** means non-SMS-based authentication methods including keystroke patterns, device fingerprinting, and authenticator apps.
- e.) **1326 Hotline** refers to the national cybercrime assistance portal operated by the Cybercrime Investigation and Coordinating Center (CICC).

SECTION 4. Senior Citizen Cyber Protection Program (SCCPP). – The State shall institutionalize the Senior Citizen Cyber Protection Program (SCCPP), a coordinated initiative led by the Cybercrime Investigation and Coordinating Center (CICC), Department of Information and Communications Technology (DICT), Philippine National Police – Anti-Cybercrime Group (PNP-ACG), National Bureau of Investigation – Cybercrime Division (NBI-CCD), *Bangko Sentral ng Pilipinas* (BSP), Department of Social Welfare and Development (DSWD), and Local Government Units (LGUs).

The SCCPP shall:

- a.) Promote digital literacy and cyber-safety awareness among senior citizens, including the deployment of multilingual modules across Filipino, Cebuano, Ilocano, Hiligaynon, and other languages;
- b.) Facilitate rapid reporting, investigation, and enforcement of online crimes affecting seniors, with age-appropriate channels;
- c.) Implement interoperable digital systems across participating agencies and financial institutions to ensure seamless data-sharing, timely alerts, and coordinated response for fraud prevention, preservation of evidence, and restitution;
- d.) Establish a monitoring and trend-analysis unit to detect emerging scams targeting elders and disseminate advisories to stakeholders, including LGUs, banks, and civil-society organizations; and
- e.) Provide technical support and guidance to Senior Cyber-Fraud Desks and SCSTs to enhance localized assistance.

SECTION 5. Qualified Circumstance: Elder-Targeted Online Fraud. – When the victim of any cybercrime, *estafa*, identity theft, or online financial fraud is a senior citizen, the penalty shall be **imposed one (1) degree higher** than that provided under the applicable law.

This provision shall apply to:

- a.) Article 315 and 318 of the Revised Penal Code (*estafa* and deceit);
- b.) R.A. 10175 (Cybercrime Prevention Act);
- c.) R.A. 8792 (E-Commerce Act);
- d.) R.A. 8484 (Access Devices Regulation Act);
- e.) R.A. 11765 (Financial Consumer Protection Act);
- f.) Acts punishable under R.A. 11934 (SIM Registration Act); and
- g.) Other laws involving digital fraud or unauthorized financial transactions.

SECTION 7. Mandatory Reimbursement for Senior Victims of Online Financial Fraud. – Financial service providers shall promptly reimburse senior citizens who fall victim to online financial fraud and to comply with all procedures necessary to ensure immediate investigation, evidence preservation, and coordinated action among relevant agencies: viz.:

- a.) **Obligation of Financial Institutions** – Banks, e-wallet providers, and other financial service entities shall refund senior citizens who fall victim to online scams, cyber-enabled fraud, or unauthorized account access within fifteen (15) calendar days from receipt of the complaint. Reimbursement shall be made unless the financial service provider can demonstrate clear negligence on the part of the senior.
- b.) **Interoperable Reporting and Verification** – Financial institutions shall use interoperable digital channels connected to the SCCPP, Senior Cyber-Fraud Desks, and LGU-based SCSTs to:
 - 1. Verify complaints in coordination with law enforcement;
 - 2. Access relevant transaction logs and records securely; and
 - 3. Coordinate rapid freezing or reversal of suspicious transactions to prevent further loss.
- c.) **Rapid Evidence Preservation and Asset Freezing** – Upon receipt of a senior citizen complaint, the following shall apply:
 - 1. Investigators from PNP-ACG or NBI-CCD shall file preservation orders within twenty-four (24) hours;
 - 2. Banks and telecommunication providers must preserve relevant data within seventy-two (72) hours;
 - 3. The Anti-Money Laundering Council (AMLC) may issue fund freezing orders within twenty-four (24) hours to secure proceeds of fraud.
- d.) **Cross-Agency Coordination** – The SCCPP shall ensure that all data, evidence, and case information are interoperable among relevant agencies, including:
 - 1. Law enforcement (PNP-ACG, NBI-CCD)
 - 2. Financial institutions and e-wallet providers
 - 3. AMLC
 - 4. LGU-based SCSTs
 - 5. Department of Social Welfare and Development (DSWD) for supporting senior victims
- e.) **Consumer Awareness and Assistance** – Senior citizens shall be provided with clear, age-appropriate instructions on reporting fraud and filing reimbursement claims, with the support of SCSTs, Senior Cyber-Fraud Desks, and SCCPP coordinators.

The burden of proof shall always be on the FSP to show absence of system failure, lack of negligence on its part, or active participation of the senior in the fraudulent activity.

SECTION 8. Senior Cyber-Fraud Desks in PNP and NBI. - All PNP stations and all NBI district offices shall establish **Senior Cyber-Fraud Desks**, staffed by personnel trained in:

- a.) Handling online scam complaints from elders;
- b.) Rapid evidence preservation;
- c.) Filing of preservation and freeze orders;
- d.) Trauma-informed interviewing;
- e.) Video-conferencing procedures for elderly witnesses.
- f.) Ensuring interoperability of records and reports with financial institutions, AMLC, and other government agencies; and
- g.) Conducting outreach and education on digital safety practices for seniors.

The PNP and NBI shall maintain 24/7 hotlines dedicated to senior citizens and shall coordinate directly with CICC's 1326 system.

SECTION 9. Immediate Data Preservation and Asset Freezing. – Upon receipt of a senior citizen’s complaint:

- a.) Data Preservation Orders under Sec. 14 of R.A. 10175 must be requested by investigators within 24 hours;
- b.) Banks, e-money issuers, and telecommunication companies must preserve data within 72 hours;
- c.) Investigators shall promptly file for a freeze order with the Anti-Money Laundering Council (AMLC) to prevent dissipation of fraud proceeds.

Failure by a bank, telecommunication company, or digital platform to comply with preservation directives shall constitute a violative act punishable by administrative sanctions.

SECTION 10. Digital Evidence Assistance for Elders. - LSWDOs, Public Attorneys, and accredited NGOs shall assist senior citizens in:

- a.) Screenshot and metadata preservation;
- b.) Drafting affidavits of complaint;
- c.) Online filing of cybercrime complaints;
- d.) Preparation of civil claims for restitution or small claims;
- e.) Securing notarization.

SECTION 11. Cyber-Safe Seniors Academy. – The DICT, in coordination with CICC, shall produce **digital-literacy modules in Filipino, Cebuano, Ilocano, Hiligaynon, and other major languages**, covering:

- a.) OTP safety and password hygiene
- b.) Identifying fake investment platforms
- c.) Avoiding romance and emergency scams
- d.) Safe use of e-wallets
- e.) Device updating and antivirus basics
- f.) Social-media privacy settings
- g.) Reporting steps using 1326 and PNP-ACG portals

DICT shall partner with telecommunication companies to provide zero-rated access to these materials.

SECTION 12. Modern Authentication Requirements for FSPs. – Within twelve (12) months of the effectivity of this Act, FSPs must:

- a.) Transition from SMS OTPs to behavioral-biometric or authenticator-app–based Multi-factor Authentication (MFA);
- b.) Activate automated fraud-gain detection for suspicious pension transactions;
- c.) Hold questionable transfers involving seniors for at least 24 hours pending verification; and
- d.) Maintain a “Senior Fraud Early Warning System.”

SECTION 13. LGU-based Senior Cyber Support Teams (SCSTs). – LGUs shall establish **Barangay Senior Cyber Support Teams (SCSTs)** composed of trained volunteers, barangay IT officers, Sangguniang Kabataan representatives, and senior citizens’ organizations. The teams shall:

- a.) Conduct community-level cyber-safety coaching;
- b.) Help seniors report online scams through interoperable channels linking SCSTs, SCCPP, and Senior Cyber-Fraud Desks;
- c.) Serve as the local liaison for cross-agency coordination in preventing, investigating, and prosecuting online crimes targeting seniors.

SECTION 14. Reporting Obligations of Telecommunication Companies and Digital Platforms. – Telecommunications firms and social-media platforms shall:

- a.) Disable confirmed scam-linked accounts within 24 hours of validated report;
- b.) Maintain real-time channels with CICC for automated scam-flagging;
- c.) Block identified phishing domains targeting elders; and
- d.) Submit quarterly reports to DICT on scam trends involving senior users.

SECTION 15. Inter-Agency Data Sharing and Enforcement. – The CICC shall maintain an **Elder Cyber-Fraud Database** accessible to:

- a.) PNP-ACG
- b.) NBI-CCD
- c.) BSP
- d.) AMLC
- e.) DSWD
- f.) DICT
- g.) Securities and Exchange Commission (SEC)

This shall include typologies, offender profiles, modus trends, and case resolutions, subject to the Data Privacy Act.

SECTION 15. Interoperability Principle. - All programs, desks, and teams under this Act shall adhere to the **principle of interoperability**, ensuring that digital platforms, databases, and reporting systems of government agencies, financial institutions, and LGUs:

- a.) Seamlessly exchange relevant data for timely detection and prevention of online scams;
- b.) Facilitate rapid coordination for investigation, asset freezing, and restitution; and
- c.) Maintain privacy, security, and confidentiality of senior citizens' personal information in accordance with the Data Privacy Act (R.A. 10173).

SECTION 16. Penalties. - Any person who commits online scams, cyber fraud, identity theft, or digital exploitation **against a senior citizen** shall suffer:

- a.) The penalty one degree higher than that provided in the underlying offense; and
- b.) Civil liability, including restitution, actual damages, moral damages, exemplary damages, and attorney's fees;
- c.) Permanent disqualification from handling financial accounts or ICT-related positions, if the offender acted in a fiduciary or professional capacity.

SECTION 17. Funding. – The amount necessary for initial implementation shall be charged against current appropriations of the concerned agencies. Thereafter, funding shall be included in the annual General Appropriations Act.

SECTION 18. Implementing Rules and Regulations. – Within **ninety (90) days** from effectivity, CICC, DICT, BSP, PNP, NBI, and DSWD shall jointly promulgate the rules for the effective implementation of this Act.

SECTION 19. Separability Clause. – If any part of this Act is declared unconstitutional, the remainder shall remain valid and effective.

SECTION 20. Repealing Clause. – All laws, orders, or regulations inconsistent with this Act are hereby repealed or modified accordingly.

SECTION 21. Effectivity Clause. – This Act shall take effect fifteen (15) days after its publication in the *Official Gazette* or in a national newspaper of general circulation.

Approved,