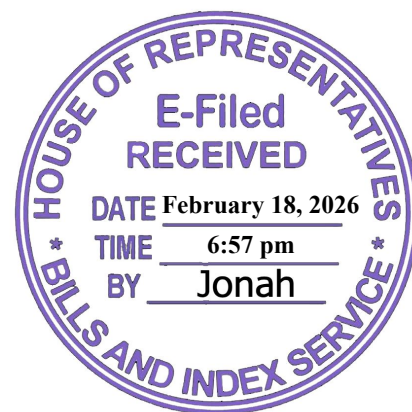


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Constitution Hills, Quezon City

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 7890



Introduced by 2nd District of Iloilo Representative
HON. KATHRYN JOYCE F. GORRICETA, M.D.

AN ACT
PENALIZING ONLINE FRAUD, DECEPTIVE DIGITAL PRACTICES, AND
MALICIOUS INTERNET ACTIVITIES, AND FOR OTHER PURPOSES

EXPLANATORY NOTE

The Constitution affirms, under Article II, Section 5, the duty of the State to protect life, liberty and property, and under Article XVI, Section 9, the obligation to safeguard consumers against deceptive, unfair and fraudulent business practices. These mandates now extend decisively into the digital sphere where the rapid expansion of e-commerce, social media, mobile payments and online marketplaces has transformed how Filipinos conduct business and interact with one another.

However, this transformation has been accompanied by an alarming rise in online fraud and malicious internet activities. The exponential growth of internet use has created unprecedented opportunities for online transactions but also enabled a surge of schemes that inflict financial loss, reputational damage, emotional distress and psychological harm on unsuspecting individuals. Among the most prevalent are online selling scams, fake investment solicitations, phishing and spoofing schemes, impersonation of private individuals or institutions and harmful forms of so-called “online pranking” that are intentionally designed to humiliate, deceive, coerce or defraud victims. These acts increasingly target minors, senior citizens, persons with disabilities and other vulnerable sectors.

Recent data makes the scale of this threat unmistakable. According to the Cybercrime Investigation and Coordinating Center (CICC), 10,004 cybercrime complaints were recorded in 2024, more than triple the 3,317 cases reported in 2023. Of these, 3,242 cases involved online fraud while 3,534 cases were classified as consumer fraud, including non-delivery of purchased goods, fake advertisements and deceptive online transactions. Losses attributed to online scams in the same year approached ₱198 million, representing only reported cases and likely understating the true level of victimization.

These risks are intensified by accelerating digital adoption. Based on the 2024 National ICT Household Survey conducted by the Philippine Statistics Authority and DICT, 48.8 percent of all households, or around 13.56 million homes, now have internet access, up sharply from only 17.7 percent in 2019. In the National Capital Region, more than 90 percent

of individuals aged ten and above now own a smartphone. This widespread connectivity, while beneficial for economic and social participation, has significantly increased exposure to online deception. Studies by the Philippine Institute for Development Studies show that one in four Filipinos has experienced a cyber incident ranging from phishing attempts to fraudulent solicitation. Monitoring reports from the National Privacy Commission and the National Cybersecurity Plan further highlight increasing incidents of identity theft, data breaches, reputational attacks and emotional harm triggered by malicious online behavior.

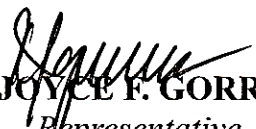
Despite the existence of laws such as the Cybercrime Prevention Act (RA 10175) and the Anti-Financial Account Scamming Act (RA 11981), substantial gaps remain. Many digital offenses, particularly those that involve fraudulent online selling, impersonation without account intrusion, malicious “pranks” intended to cause harm, deceptive solicitations, fabricated digital identities and manipulative online content, are not adequately covered by existing statutes. These activities often escape prosecution because they do not neatly fall under hacking, cybersex or the limited set of punishable acts enumerated in older legislation.

This measure seeks to fill these gaps by defining, prohibiting and penalizing various forms of online fraud and malicious internet activities that exploit digital platforms, social media algorithms or electronic communications. It specifically targets online selling scams and fraudulent commercial transactions, deceptive digital solicitations and fabricated advertisements, impersonation of individuals or institutions for financial or malicious gain, phishing, spoofing and similar techniques aimed at stealing personal or financial data and malicious online pranking that inflicts psychological, reputational or financial harm.

The bill likewise enhances inter-agency coordination among the Department of Information and Communications Technology (DICT), the Department of Trade and Industry (DTI), the Philippine National Police Anti-Cybercrime Group (PNP-ACG) and the National Bureau of Investigation Cybercrime Division (NBI-CCD) to ensure robust enforcement, digital forensics capability and efficient prosecution of offenders. Digital platforms operating in the Philippines are also encouraged to establish accessible reporting mechanisms and to cooperate lawfully with enforcement agencies.

By modernizing the country’s legal framework against digital deception, protecting citizens from emerging online harms and strengthening accountability in the digital marketplace, this measure fulfills the State’s constitutional responsibility to uphold consumer welfare, protect property and dignity and secure the well-being of Filipinos in an increasingly interconnected society.

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


KATHRYN JOYCE F. GORRICETA, M.D.
Representative
2nd District of Iloilo

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Constitution Hills, Quezon City

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 7890

Introduced by 2nd District of Iloilo Representative
HON. KATHRYN JOYCE F. GORRICETA, M.D.

AN ACT
PENALIZING ONLINE FRAUD, DECEPTIVE DIGITAL PRACTICES, AND
MALICIOUS INTERNET ACTIVITIES, 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 “*Anti-Online Fraud and Malicious Internet Activities Act*.”

SEC. 2. **Declaration of Policy.** The State shall safeguard individuals and institutions from online fraud, deceptive digital practices, and malicious internet activities. It shall promote a secure and trustworthy digital ecosystem that upholds responsible online conduct, supports legitimate e-commerce, and protects the public from psychological, reputational, and financial harm.

SEC. 3. **Definition of Terms.** For purposes of this Act:

- a. *Online Fraud* — any act, scheme, or device carried out through digital or electronic means intended to deceive, misrepresent, or defraud individuals or entities for personal, financial, or material gain, whether completed or attempted.
- b. *Online Selling Scam* — any deceptive act involving the sale of goods or services online, including non-delivery, delivery of materially different or defective items, false representation of identity, or use of fabricated transaction proofs.
- c. *Malicious Online Pranking* — the intentional creation, transmission, or dissemination of false, harmful, humiliating, or distressing content through digital platforms for the purpose of causing emotional harm, reputational damage, public humiliation, financial loss, or disruption of daily activities.
- d. *Digital Platform* — any website, application, social media service, marketplace, communication service, or online system accessible through the internet.

- e. *Phishing and Spoofing* — fraudulent techniques used to deceive individuals into divulging personal information, login credentials, financial data, or other sensitive information through imitation, manipulation, or misrepresentation of legitimate entities.

SEC. 4. ***Prohibited Acts.*** The following acts shall be unlawful:

- a. Engaging in online selling scams or other fraudulent commercial transactions conducted through digital platforms.
- b. Creating or conducting malicious online pranks that cause or are reasonably expected to cause emotional distress, reputational damage, financial loss, or harassment.
- c. Impersonating or falsely representing an individual, organization, or institution to solicit money, property, services, or personal data.
- d. Disseminating fabricated, misleading, or deceptive online advertisements or promotional content.
- e. Conducting phishing, spoofing, false identity fabrication, or any other deceptive digital practices aimed at obtaining personal, financial, or sensitive information.
- f. Knowingly facilitating, aiding, or abetting the commission of any of the acts defined under this Act.

SEC. 5. ***Penalties.***

- a. Any person found guilty of committing any prohibited act under this Act shall suffer the penalty of prisión correccional (six months and one day to six years) and/or a fine of ₱50,000 to ₱500,000, depending on the gravity and extent of damage.
- b. When the offender is a juridical person, the responsible officers, directors, managers, or agents who participated in, authorized, or tolerated the unlawful acts shall be held criminally liable.
- c. When the offense results in large-scale fraud, affects three (3) or more victims, involves government financial assistance or public funds, or compromises critical personal data, the penalty shall be imposed in its maximum period.
- d. When the victim is a minor, senior citizen, pregnant woman, or a person with disability, the penalty shall likewise be imposed in its maximum period.
- e. The court may further order restitution, return of unlawfully obtained property, and payment of actual damages.

SEC. 6. ***Jurisdiction.*** This Act shall apply to:

- a) Offenses committed within the Philippines; and
- b) Offenses committed outside the Philippines when any of the elements, effects, or damages are experienced within Philippine territory, or when the victim is a Filipino citizen.

SEC. 7. ***Reporting Mechanism.*** — Digital platforms operating in the Philippines shall establish accessible reporting systems for suspected violations of this Act and shall cooperate with law enforcement agencies upon lawful request.

SEC. 8. ***Implementing Rules and Regulations (IRR)***. Within sixty (60) days from the effectivity of this Act, the Department of Information and Communications Technology (DICT), in consultation with the Department of Justice (DOJ), the Department of Trade and Industry (DTI), the National Privacy Commission (NPC), the National Telecommunications Commission (NTC), and relevant stakeholders, shall promulgate the implementing rules and regulations necessary to carry out the provisions of this Act.

SEC. 9. ***Appropriations***. The funds necessary for the effective implementation of this Act shall be included in the annual General Appropriations Act.

SEC. 10. ***Separability Clause***. If any part or provision of this Act is declared unconstitutional or invalid, the remaining portions not affected shall remain in full force and effect.

SEC. 11. ***Repealing Clause***. All laws, decrees, issuances, or rules inconsistent with this Act are hereby amended or repealed accordingly.

SEC. 12. ***Effectivity***. This Act shall take effect fifteen (15) days after publication in the Official Gazette or in a newspaper of general circulation.

Approved,