REPUBLIC OF THE PHILIPPINES

HOUSE OF REPRESENTATIVES

Quezon City

EIGHTEENTH CONGRESS

Third Regular Session

House Bill No. **10412**

Introduced by **MAGDALO Party-List Representative**

HON. MANUEL DG. CABOCHAN III

EXPLANATORY NOTE

The emergence of digital technology has transformed nearly every aspect of modern life. People can now easily integrate information and communication technologies at home, work, education, and recreation. It has revolutionized work, travel, shopping, entertainment, and banking in recent decades. Digital platforms such as online banking are changing the traditional relationships between clients, workers, and employers. Bank users can now check their incoming and outgoing payments remotely, as well as arrange bill payments and money transfers.

The COVID-19 pandemic has immensely forced people to shift to the use of online platforms to make transactions. With this, it gave rise to heightened activity by cybercriminals. Citing data from the Philippine National Police Anti-Cybercrime Group (PNP-ACG), 869 online scams were recorded from March to September 2020, 37% higher than the 633 incidents recorded in the same period in 2019.[1] Further, the impact of cybercrime is expected to reach $6 trillion in 2021 and rise to as much as $10.5 trillion annually by 2025. Crime activities such as phishing, smishing, vishing

[1] Business World. Cybercrime to increase further as transactions shift online. Information retrieved from https://www.bworldonline.com/cybercrime-to-increase-further-as-transactions-shift-online/. Dated March 8, 2021

and other online fraud schemes target bank clients, credit card holders, e-wallet accounts, online shopping, and other uses of online finance services.

This proposed measure seeks to protect all persons from falling prey to various cybercrime activities by regulating and prohibiting the use of bank accounts and electronic (e-wallets) for unusual and suspicious financial activities. It shall penalize money mules and social engineering schemes leading to illicit online financial activities. It is paramount, therefore, that digital financial services must be regulated to ensure the safety of the public and to strengthen the financial system's defense against cybercriminals.

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

MANUEL DG. CABOCHAN III
Representative
Magdalo Para Sa Pilipino Party-List

REPUBLIC OF THE PHILIPPINES

HOUSE OF REPRESENTATIVES

Quezon City

EIGHTEENTH CONGRESS

Third Regular Session

House Bill No. **10412**

Introduced by **MAGDALO Party-List Representative**

HON. MANUEL DG. CABOCHAN III

AN ACT

REGULATING THE USE OF BANK ACCOUNTS AND E-WALLETS AND PROHIBITING THE USE THEREOF FOR UNUSUAL AND SUSPICIOUS FINANCIAL ACTIVITY

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

SECTION 1*. Short Title.*– This Act shall be known as the "Bank Account and E-wallet Regulation Act".

Sec. 2. *Declaration of Policy.*– The State recognizes the vital role of both banks and the general public in promoting and maintaining a stable and efficient financial system. The State also acknowledges that in the advent of electronic commerce (e-commerce) and digital banking, there is a need to protect the public from cybercriminals and criminal syndicates who target bank accounts and e-wallets and lure account holders to aid them in perpetrating fraudulent activities. It shall be the policy of the State to undertake measures to protect all persons from falling prey to the various cybercrime schemes by regulating and prohibiting the use of bank

accounts and electronic wallets (e-wallets) for unusual and suspicious financial activities. Furthermore, due to the deleterious effect on the economy, the State declares that the commission of certain crimes under this Act when done in bulk or in large scale is a form of economic sabotage and a heinous crime and shall be punishable to the maximum level allowed by law.

Sec. 3. *Definition of Terms.*– For purposes of this Act, the following terms are hereby defined as follows:

(a) *Account Takeover* refers to a form of identity theft and fraud, where a malicious third party successfully gains access and control of a user's financial accounts;

(b) *Bulk Emailing/Mass Electronic Mailing* refers to the act of sending an electronic mail (email) in mass, with at least ten (50) or more recipients;

(c) *Entity* refers to natural or juridical persons, including corporations, partnerships, associations, organizations, joint ventures, government agencies or instrumentalities, Government-Owned and Controlled Corporations (GOCCs), or any other legal entity, whether for profit or not-for-profit;

(d) *Electronic Wallet (E-wallet)* refers to a software or application which allows the user to store money for any future online transaction;

(e) *Money Mule* refers to any person who electronically receives, acquires, and transfers or withdraws money, funds, or proceeds derived from suspicious activities, social engineering schemes or other crimes/offenses committed through the use of information and communications technology, on behalf of others, in exchange for commission or fee, and those who commit the acts under Section 4 (a) of this Act;

(f) *Other Financial Accounts* refer to new or emerging forms of financial accounts other than bank accounts and e-wallets;

(g) *Phishing* refers to a social engineering scheme of posing as a legitimate or trusted entity, or as a representative of a legitimate or trusted entity mainly through electronic communication in order to obtain sensitive identifying information of another by illegally accessing an individual's online account;

(h) *Sensitive Identifying Information* refers to any information that can be used to access an individual's financial accounts such as, but not limited to, usernames, passwords, bank account details, credit card, debit card, and e-wallet information, among other electronic credentials;

(i) *Social Engineering Scheme*, in the context of information security, refers to the use of deception to manipulate individuals into divulging sensitive identifying information that may be used to gain access to an individual's financial accounts, regardless of whether or not it will result in monetary loss to the account holder. This includes phishing and any of its variations such as but not limited to vishing, smishing, as well as other similar forms of deception;

(j) *Suspicious Activity* refers to any online transaction, regardless of amount, where any of the following circumstances exists:

(1) There is no underlying legal or trade obligation, purpose or economic justification;

(2) The number of online transactions, amount involved, or any circumstance relating to the activity is observed to be unusual or deviates from the profile of the client or the client's past transactions;

(3) The transaction is in any way related to an unlawful activity or to a social engineering scheme or cybercrime that is about to be, is being or has been committed;

(4) Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to aid the perpetrators of an unlawful activity, social engineering scheme or cybercrime; and

(5) Any transaction that is similar, analogous or identical to any of the foregoing.

SEC. 4. *Prohibited Acts.*– The following acts shall constitute an offense punishable under this Act:

(a) Money Mule. It shall be prohibited for any person to act as a money mule as defined under this law.

The following acts shall also constitute as an offense:

(1) Opening a bank or e-wallet account and using or allowing the use thereof, to receive and transfer or withdraw proceeds derived from a suspicious activity or cybercrime;

(2) Opening a bank or e-wallet account under a fictitious name or using the identity or identification documents of another to receive and transfer or withdraw proceeds derived from a suspicious activity or cybercrime;

(3) Buying or renting a bank or e-wallet account for the purpose of receiving and transferring or withdrawing proceeds derived from a suspicious activity or cybercrime;

(4) Selling a bank or e-wallet account for the purpose of receiving and transferring or withdrawing proceeds derived from a suspicious activity or cybercrime;

(5) Account takeover or using or borrowing a bank or e-wallet account for the purpose of receiving and transferring or withdrawing proceeds derived from a suspicious activity or cybercrime;

(6) Recruiting, enlisting, contracting, hiring or inducing any person to electronically obtain, receive, acquire, and transfer or withdraw money, funds, or proceeds derived from a suspicious activity or cybercrime. Recruitment of money mules when committed by a syndicate or in large scale shall be considered as an offense involving economic sabotage.

(b) Social Engineering Schemes. Any person performing any social engineering schemes as defined under Section 3, including phishing and any variations thereof, shall be penalized under this Act.

(c) Economic Sabotage. Any offense defined under this Section shall be considered as an offense involving economic sabotage when any of the following circumstances is present:

(1) The offense was committed by a syndicate;

(2) The offense was committed in large scale; or

(3) The offense was committed by way of bulk email or mass mail.

For this purpose, an act shall be deemed committed by a syndicate if the offense was carried out by a group of three (3) or more persons conspiring or confederating with one another. Meanwhile, an act shall be deemed committed in large scale if the offense was committed against three (3) or more persons individually or as a group.

Sec. 5. *Other Offenses*.– The acts involving or having relation to the following shall also constitute an offense:

(a) Aiding or Abetting a Money Mule. — Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable; and

(b) Attempt in the commission of a crime. — Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

Sec. 6. *Liability Under Other Laws.*– A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.

Sec. 7. *Penalties*.– Any person found guilty of the punishable act under Section 4(A) shall be punished with imprisonment of prision correccional or a fine of at least One hundred thousand pesos (PhP100,000.00) but not exceeding Two hundred thousand pesos (PhP200,000.00), or both,

Any person found guilty of any of the punishable acts enumerated in Section 4(B) shall be punished with imprisonment of prision mayor or a fine of at least Two hundred thousand pesos (PhP200,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00), or both.

Provided, however, That the maximum penalty shall be imposed if the target or victim/s of the social engineering scheme is or includes a senior citizen aged sixty (60) years old or above at the time the offense was committed or attempted.

Any person found guilty of any of the offenses that constitutes economic sabotage under Section 4(C) shall be punished with life imprisonment and a fine of not less than One million pesos (PhP1,000,000.00) but not more than Five Million Pesos (PhP500,000.00).

Sec. 8. *Jurisdiction*.– The Regional Trial Court, designated as cybercrime court, shall have jurisdiction over any violation of the provisions of this Act, including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

Sec. 9. *General Principles Relating to International Cooperation*.– All relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense, shall be given full force and effect.

Sec. 10. *Enforcement*.– The NBI and PNP shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The cybercrime unit or center established under Section 10 of Republic Act No. 10175 shall exclusively handle all cases involving violations of this Act.

Sec. 11. *Response to Consumers*.– Banks, Non-Bank Financial Institutions, and other pertinent Bank and Non-Bank Institutions shall immediately and effectively respond to all complaints related to social engineering attacks other cybercrimes perpetrated upon consumers. They shall comprehensively investigate each case, provide continuous updates to consumers, coordinate with the proper authorities, and exhaust all means to ensure that victims are able to recover their monetary loss, if

any. The said institutions shall likewise institute measures to strengthen their online platforms, payment systems, and data security, among others.

Sec. 12. *Appropriations*.– The amount needed for the initial implementation of this Act shall be taken from the current year's appropriations of the concerned agencies. Thereafter, such sums as may be necessary for its continued implementation shall be included in the annual General Appropriations Act.

Sec. 13. *Implementing Rules and Regulations*.– Within sixty (60) days from the effectivity of this Act, the Bangko Sentral ng Pilipinas (BSP), Department of Justice (DOJ), Department of Information and Communications Technology (DICT), National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall promulgate the rules and regulations to effectively implement the provisions of this Act.

These agencies shall formulate an "Anti-Scam/Financial Fraud Roadmap" which shall include detailed measures on, among others, education and information dissemination on financial scams and its prevention; enhanced detection, reporting, and prosecution of persons behind money mules, social engineering schemes, and other financial cybercrimes; and the training of responsible officers and personnel to ensure the effective enforcement and prosecution of cases under this Act.

Sec. 14. *Separability Clause*.– If any portion or provision of this Act is subsequently declared invalid or unconstitutional, other provisions hereof which are not affected thereby shall remain in full force and effect.

Sec. 15. *Repealing Clause*.– All other laws, acts, presidential decrees, executive orders, presidential proclamations, issuances, rules and regulations, or parts thereof which are contrary to or inconsistent with any of the provisions of this Act are hereby repealed, amended or modified accordingly.

Sec. 16. *Effectivity*.– This Act shall take effect fifteen (15) days after its publication in the *Official Gazette* or in any newspaper of general circulation.

Approved,