NINETEENTH CONGRESS OF THE REPUBLIC OF THE PHILIPPINES
Second Regular Session

SENATE

S.B. No. 2306

Introduced by **SENATOR JOEL VILLANUEVA**

AN ACT
DEFINING AND PENALIZING FRAUDULENT ACTIVITIES INVOLVING BANK ACCOUNTS, E-WALLETS, AND OTHER FINANCIAL ACCOUNTS, AND FOR OTHER PURPOSES

EXPLANATORY NOTE

The COVID-19 pandemic has highlighted the importance of digitalization for economic and social resilience. With mobility and face-to-face interactions and activities restricted, many Filipinos have turned to online and digital banking methods to conduct their personal and business transactions. According to the Bangko Sentral ng Pilipinas (BSP), the number of Filipinos with access to banks and electronic money channels has grown to 41 million as of October 2021, from about 21 million in 2019.[1] The central bank said 3.6 million new basic deposit accounts were opened between the end of 2019 and late 2021, while e-money accounts increased by 16.8 million during the same period.[2]

However, with the fast advancement of technologies and continued evolution of banking and electronic payment methods, fraudulent activities involving bank accounts, electronic wallets (e-wallets), and other financial accounts have also increased. The BSP reported that complaints related to the use of internet banking and mobile banking constitute 45.2% of the total complaints they received in 2021.[3] From 2020 to 2021, 42,456 complaints in relation to financial fraud, including account

[1] Inquirer.net. *41 million Filipinos now have banking, e-money access.* 17 February 2022. Available at https://business.inquirer.net/341084/41m-filipinos-now-have-banking-e-money-access. Accessed on 03 July 2023.
[2] *Ibid.*
[3] BSP. *Opening Statement of BSP Governor Benjamin E. Diokno during the Senate Deliberation on the Proposed Financial Consumer Protection Act.* 17 January 2022. Available at https://www.bsp.gov.ph/SitePages/MediaAndResearch/SpeechesDisp.aspx?ItemId=893. Accessed on 03 July 2023.

takeover or identity theft, phishing, and other social engineering schemes were elevated to the BSP Consumer Assistance Mechanism.[4]

Hence, this bill seeks to protect consumers from syndicates and cyber criminals who target bank accounts, e-wallets, and other financial accounts, or lure account holders into committing fraudulent activities. This measure also prohibits money mules, account takeover, phishing, and other social engineering schemes and declares the large-scale commission of such crimes as a form of economic sabotage. Further, banks and other financial institutions shall be mandated to immediately and effectively respond to all consumer complaints related to fraudulent activities involving their financial accounts, and to ensure that measures are instituted to strengthen their online platforms, payment systems, and data security, among others.

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

JOEL VILLANUEVA

[4] *Ibid.*

NINETEENTH CONGRESS OF THE REPUBLIC OF THE PHILIPPINES
Second Regular Session

SENATE

S.B. No. 2306

Introduced by **SENATOR JOEL VILLANUEVA**

AN ACT
DEFINING AND PENALIZING FRAUDULENT ACTIVITIES INVOLVING BANK ACCOUNTS, E-WALLETS, AND OTHER FINANCIAL ACCOUNTS, AND FOR OTHER PURPOSES

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 "*Financial Account Fraud Prevention Act.*"

SEC. 2. ***Declaration of Policy.*** – The State recognizes the vital role of banks, payment service providers, and the general banking public in promoting and maintaining a stable and efficient financial system. The State also acknowledges that in the advent of electronic commerce and digital banking, there is a need to protect the public from cyber criminals and criminal syndicates who target bank accounts and e-wallets or lure account holders into perpetrating fraudulent activities.

It shall therefore be the policy of the State to undertake measures to protect all persons from falling prey to the various cybercrime schemes by regulating the use of bank accounts, electronic wallets (e-wallets), and other financial accounts, and preventing their use in fraudulent activities. Furthermore, due to the deleterious effect on the economy, the large-scale commission of certain crimes under this Act shall be declared 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) Account Owner – refers to the owner/s of a bank account, e-wallet, or other financial account, as registered with the bank or financial institution;

c) Bank Account – refers to an interest or non-interest bearing deposit, trust, investment, and other transaction account maintained with a bank or a financial institution;

d) Bulk or Mass Messaging – refers to the act of sending messages by means of electronic mail (email), short messaging service (SMS), chat message, or other written, digital or electronic form of communication to an aggregate or total of fifty (50) recipients or more, counted from the first to the last act of sending;

e) Cybercrime – refers to the punishable acts and offenses enumerated under Section 4 of Republic Act No. 10175, otherwise known as the Cybercrime Prevention Act of 2012;

f) Electronic Wallet (e-wallet) – refers to an electronic account which stores monetary value through a software or application, which is pre-funded to enable the processing of financial transactions including, but not limited to, payments or fund transfers to other individuals or entities, top-ups or cash-in, and/or withdrawals, among others. Examples of e-wallet include electronic money or virtual asset accounts stored in mobile phones or web-based applications;

g) 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 body or structure, whether for profit or not-for-profit;

h) Money Mule – refers to any person who obtains, receives, acquires, transfers, or withdraws money, funds, or proceeds derived from crimes, offenses, or social engineering schemes on behalf of others, in exchange for a commission or fee, and those who commit the acts under Section 4 (a) of this Act. For this purpose, money, funds, or proceeds shall include, but not be limited to, coins or currency of legal tender of the Philippines or another jurisdiction, electronic money, virtual assets, securities or negotiable instruments, other monetary or financial instrument, or all things which are or may be the object of appropriation;

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

j) Phishing – refers to a social engineering scheme whereby a person falsely represents himself/herself to another person as a legitimate institution, entity, or a representative thereof, for the purpose of obtaining the latter's sensitive identifying information and/or accessing and transacting the latter's bank, e-wallet, or other financial account;

k) 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;

l) Social Engineering Scheme – refers to the use of deception or other fraudulent means to obtain confidential or personal information, including sensitive identifying information, of another individual or entity. Social engineering schemes may be committed in-person or through various media or platforms including, but not limited to:

1) Electronic mail;
2) Short message service, text messages, or other message services;
3) Social media sites and applications;
4) Websites;
5) Telephone or voice calls;
6) Mobile or other electronic applications;
7) Advertisements; or
8) Search engines.

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 Act. The following acts shall also constitute as an offense:

1) Opening a bank account, e-wallet account, or other financial account and using or allowing the use thereof to receive, transfer, or withdraw proceeds derived from crimes, offenses, or social engineering schemes;
2) Opening a bank account, e-wallet, or other financial account under a fictitious name or using the identity or identification documents of another person or entity to receive, transfer, or withdraw proceeds derived from crimes, offenses, or social engineering schemes;
3) Buying or renting a bank account, e-wallet account, or other financial account for the purpose of receiving, transferring, or withdrawing proceeds derived from crimes, offenses, or social engineering schemes;
4) Selling a bank account, e-wallet, or other financial account for the purpose of receiving, transferring, or withdrawing proceeds derived from crimes, offenses, or social engineering schemes;
5) Borrowing and using a bank account, e-wallet account, or other financial account for the purpose of receiving, transferring, or withdrawing proceeds derived from crimes, offenses, or social engineering schemes; and
6) Recruiting, enlisting, contracting, hiring, or inducing any person to act as a money mule;

b) Phishing and Social Engineering Schemes. – It shall be prohibited for a person to commit phishing, including any variations thereof, and social engineering schemes, as defined under Section 3 (j) and (l) of this Act: *Provided,* That loss, damage or injury to other persons as a result of the social engineering scheme is not a necessary element of this offense, and the lack thereof may not be interposed as a defense: *Provided, further,* That if the offense was committed by way of bulk or mass messaging, the penalty to be imposed shall be one degree higher;

c) Account Takeover. – It shall be prohibited for a person to commit account takeover, as defined under Section 3(a) of this Act;

d) Economic Sabotage. – Any offense defined under this subsection 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 individual or aggregate amount involved in the offense is greater than Two Million Pesos (P2,000,000.00).

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 with one another. Further, 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) Any person who willfully abets or aids in the commission of any of the offenses enumerated under Section 4 of this Act shall be held liable; and

b) Any person who willfully attempts to commit any of the offenses enumerated under Section 4 of 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 other laws.

SEC. 7. ***Penalties.*** – Any person found guilty of the prohibited acts under Section 4(a) shall be punished with imprisonment of *prision mayor in its minimum period* and a fine of at least One Hundred Thousand Pesos (P100,000.00) but not exceeding Two Hundred Thousand Pesos (P200,000.00), or both.

Any person found guilty of any of the prohibited acts under Section 4 (b) and (c) shall be punished with imprisonment of *prision mayor in its maximum period* and a fine of at least Two Hundred Thousand Pesos (P200,000.00) but not exceeding Five Hundred Thousand Pesos (P500,000.00), or both: *Provided,* That the maximum penalty shall be imposed if the target or victim 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(d) shall be punished with life imprisonment and a fine of not less than One Million Pesos (P1,000,000.00) but not more than Five Million Pesos (P5,000,000.00).

Any person found guilty of any of the punishable acts enumerated in Section 5

shall be punished with imprisonment one (1) degree lower than that of the prescribed penalty for the offense and a fine of at least One Hundred Thousand Pesos (P100,000.00) but not exceeding Five Hundred Thousand Pesos (P500,000.00), or both.

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. For the purpose of this Act, 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 National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective enforcement of the provisions of this Act. The cybercrime unit or center established under Section 10 of Republic Act No. 10175, otherwise known as the Cybercrime Prevention Act of 2012, shall exclusively handle all cases involving violations of this Act: *Provided,* That they shall closely coordinate with the *Bangko Sentral ng Pilipinas* (BSP) and other relevant government agencies in the investigation and enforcement of cybercrime warrants and related orders.

SEC. 11. ***Duties of Banks and Financial Institutions.*** – Banks, non-bank financial institutions, and other pertinent institutions shall immediately and effectively respond to all consumer complaints related to phishing, social engineering schemes, account takeover, or other cybercrimes that are committed on their platform. They shall comprehensively investigate each case, exert reasonable efforts to assist victims in recovering their direct monetary loss, if any, provide continuous updates to consumers, and provide evidence in support of any criminal investigations or legal actions that may be initiated by the victims or legal authorities.

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

SEC. 12. ***Implementing Rules and Regulations.*** – Within sixty (60) days from the effectivity of this Act, the BSP, Department of Justice (DOJ), Department of Information and Communications Technology (DICT), NBI, and PNP shall jointly promulgate the rules and regulations to effectively implement the provisions of this Act.

These agencies shall also 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.

Additionally, a cooperative mechanism shall be established among the concerned government agencies, banks, financial and other covered institutions, private and corporate sectors, and other concerned stakeholder groups to ensure the effective prosecution of cases and enforcement of this Act.

SEC. 13. ***Appropriations.*** – The amount necessary for the effective implementation of this Act shall be included in the annual General Appropriations Act (GAA).

SEC. 14. ***Separability Clause.*** – If any provision of this Act is declared invalid or unconstitutional, the other provisions not affected by such declaration shall remain in full force and effect.

SEC. 15. ***Repealing Clause.*** – All laws, decrees, orders, and issuances, or portions thereof, which are inconsistent with 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 complete publication in the *Official Gazette* or in a newspaper of general circulation.

Approved,