NINETEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
First Regular Session)

SENATE

S. No. 2171

Introduced by Senator Jinggoy Ejercito Estrada

AN ACT
REGULATING THE USE OF BANK ACCOUNTS, ELECTRONIC WALLETS, AND OTHER FINANCIAL ACCOUNTS, PROVIDING PENALTIES THEREFOR AND FOR OTHER PURPOSES

EXPLANATORY NOTE

Owing to the restrained mobility of people due to the COVID-19 pandemic, financial consumers' behavior towards digital transactions improved and led to an uptake in the adoption of digital financial services. With this, however, came risks such as hacking incidents, phishing scams, bank account and credit card fraud, among others.

According to the *Bangko Sentral ng Pilipinas* (BSP) in 2020 and 2021, the BSP Consumer Assistance Mechanism System received 42,456 complaints from financial consumers. In 2020 hacking and other malware attacks increased by 2,324% from the previous year, while phishing other social engineering schemes increased by 302% from the previous year. For 2021, 45.2 percent of complaints received by the BSP were related to internet and mobile banking. As to the declared amounts in the complaints, for 2021 alone it was at P540 million, but the cumulative total from 2019 to 2020 amounted to P2 billion. Furthermore, while the majority of the cases have been closed, the process was long and burdensome, and for many of the complaints, the resolution was oftentimes not favorable to the consumer.

As it stands, the Philippines lags behinds its ASEAN neighbors in terms of financial inclusion, with only 56% of the adult population with a bank account in 2021. Risks with financial transactions could dampen financial consumers' confidence even more towards digital transactions, traditional banking, and the financial system in general.

This bill seeks to fully equip and empower government agencies and financial regulators to enforce measures that will address the risks and cyber threats that financial consumers are exposed to. Money muling and social engineering schemes such as phishing and vishing, are punishable offenses under this bill. While offenses committed by a syndicate, done on a large scale, or using a mass mailer shall be considered as offenses involving economic sabotage. This bill also seeks to provide financial consumers with efficient means to resolve their complaints, making it less cumbersome, more transparent, and allowing for quicker resolutions that will be more to their advantage.

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

JINGGOY EJERCITO ESTRADA

NINETEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
First Regular Session)

SENATE

S. No. 2171

Introduced by Senator Jinggoy Ejercito Estrada

AN ACT
REGULATING THE USE OF BANK ACCOUNTS, ELECTRONIC WALLETS, AND OTHER FINANCIAL ACCOUNTS, PROVIDING PENALTIES THEREFOR 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 "*Bank Accounts, Electronic Wallets, and Other Financial Accounts Regulation 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 with the increased use of electronic commerce and digital banking, there is a need to protect the public from cybercriminals and criminal syndicates who target financial accounts, electronic wallets (e-wallets), and other financial accounts, or lure account holders into perpetrating fraudulent activities. It shall therefor be the policy of the State to regulate the use of financial accounts, e-wallets, and other financial accounts.

Furthermore, due to the damaging effect on the economy, the large-scale commission of certain crimes in this Act is hereby declared a form of economic sabotage and a heinous crime and as such shall be punishable to the maximum level allowed by law.

Sec. 3. *Definition of Terms.* – As used in this Act:

a. *Account takeover* refers to a form of identity theft and fraud, where a malicious third party successfully gains access and control over a user's financial account, e-wallet, or other financial account;
b. *Bulk e-mail or mass mailer* refers to a service or software used to send electronic mail (e-mail) in mass or to fifty (50) or more emails;
c. *Electronic Wallet or E-wallet* refers to a digital value stored in a wallet as may be defined by the *Bangko Sentral ng Pilipinas* (BSP) regulations;
d. *Financial Account* refers to an interest or non-interest earning deposit, trust, investment, credit card, and other transaction account maintained with a bank, non-bank, or financial institution;
e. *Money mule* refers to any person who obtains, receives, acquires, or transfers or withdraws money, funds, or proceeds derived from crimes, offenses, or social engineering schemes, and those who commit the prohibited acts under Section 4(a) of this Act;
f. *Multi-Factor Authentication (MFA)* refers to an authentication method that requires the used to provide two (2) or more verification factors, such as something one knows, something one has, and something one is, to gain access to a resource;
g. *Other Financial Accounts* refer to the various types of accounts used for financial transactions other than bank accounts and e-wallets;
h. *Persons* refer 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;
i. *Sensitive Identifying Information* refers to any information that can be used to access an individual's financial accounts such as, usernames, passwords, bank account details, credit card, debit card, and e-wallet information among other electronic credentials; and,
j. *Social Engineering Scheme* refers to the use of deception or fraudulent means by a person to obtain confidential or personal information, including sensitive identifying information, of another person, and those acts enumerated under Section 4(b) of this Act.

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. Any person performing any of the following acts shall be considered as a money mule:
    1. Opening a financial, e-wallet, or other financial account and using or allowing the use thereof, to receive or transfer or withdraw proceeds known to be derived from crimes, offenses, or social engineering schemes;
    2. Opening a financial, e-wallet, or other financial account under a fictitious name or using the identity or identification documents of another to receive or transfer or withdraw proceeds derived from crimes, offenses, or social engineering schemes;
    3. Buying or renting a financial, e-wallet, or other financial account for the purpose of receiving or transferring or withdrawing proceeds derived from crimes, offenses, or social engineering schemes;
    4. Selling and lending a financial, e-wallet, or other financial account for the purpose of receiving or transferring or withdrawing proceeds derived from crimes, offenses, or social engineering schemes;
    5. Performing account takeover or using or borrowing a financial, e-wallet, or other financial account for the purpose of receiving or transferring or withdrawing proceeds derived from crimes, offenses, or social engineering schemes; or
    6. Recruiting, enlisting, contracting, hiring, utilizing, or inducing any person to perform the acts mentioned in items 1 to 5 of this Section.
b. *Social Engineering Schemes*. Any person performing any social engineering scheme shall be penalized under this Act. Social engineering scheme shall also be deemed committed when a person performs any of the following:
    1. Makes any communication to another person by representing oneself as a representative of a financial institution or making any false representation in order to gain the trust of others and solicit sensitive identifying information that results in account takeover; or

2. Uses electronic communication to induce or request any person to provide sensitive identifying information with the intent to defraud or injure any person.

Banks and other financial institutions shall ensure that access to their clients' accounts is protected by the highest level of security, including MFA, security redundancies, and other account-holder authentication and verification processes: *Provided*, That such security levels are proportionate and commensurate with the nature, size, and complexity of their operations. Subject to sufficient and undeniable proof resulting from a thorough investigation within a reasonable time, the failure of these institutions to exercise proper diligence shall result in immediate restitution of amounts lost to the rightful owners.

c. *Economic Sabotage*. Any offense defined under this section shall be considered as an offense involving economic sabotage when any of the following circumstances are present:

1. The offense was committed by a syndicate;
2. The offense was committed in large scale; or
3. The offense was committed using a mass mailer.

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, while 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 constitute an offense:

a. Any person who willfully aid or abets in the commission of any of the offenses enumerated in Section 4 of this Act shall be held liable; and
b. Any person who willfully attempts to commit any of the offenses enumerated in Section 4 of this Act shall be held liable.

Sec. 6. *Higher Penalty for Acts Committed Under the Revised Penal Code and Crimes Under Special Laws using Money Mule and Social Engineering Schemes.* – All crimes defined and penalized by Act No. 3815, otherwise known as the Revised Penal Code, as amended, and special laws, if committed by and through the acts as defined

under Section 4 hereof, shall be covered by relevant provisions of this Act: *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

Sec. 7. *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. 8. *Penalties*. – Any person found guilty of the punishable act under Section 4(a) hereof shall be punished with imprisonment or *prision correccional* or 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 punishable acts enumerated in Section 4(b) hereof shall be punished with imprisonment of *prision mayor* or 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, however*, 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(c) hereof 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 hereof shall be punished with imprisonment one (1) degree lower than that of the prescribed penalty for the offense or 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. 9. *Corporate Liability*. – When any of the punishable acts herein defined knowingly committed on behalf of or for the benefit of a juridical person, by a natural person who has a leading position within based on (a) a power of representation of the juridical person: *Provided*, That the act committed falls within the scope of such authority; (b) an authority to take decisions on behalf of the juridical person: *Provided*, That the act committed falls within the scope of such authority; or (c) an authority to

exercise control within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 8 hereof up to a maximum of Ten million pesos (P10,000,000.00).

Sec. 10. *Enforcement.* – The provision of Chapter IV of Republic Act No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012" shall be applicable in the enforcement of this Act: *Provided,* That in addition to the cybercrime units of the National Bureau of Investigation (NBI) and the Philippine National Police (PNP), the BSP shall have the authority to investigate cases involving violations of this Act, and to apply for cybercrime warrants and orders mentioned in Chapter IV of Republic Act No. 10175: *Provided, further,* That the BSP may request assistance of the NBI and the PNP in the investigation of cases involving violations of this Act and in the enforcement and implementation of cybercrime warrants and related orders.

The BSP shall have the authority to examine and investigate individual financial accounts, e-wallets, or other financial accounts which are involved in the prohibited acts and other offenses under Sections 4 and 5 of this Act. For this purpose, the provisions of Republic Act No. 1405, otherwise known as the "Secrecy of Bank Deposits Law", Republic Act No. 6426, as amended, otherwise known as the "Foreign Currency Deposit Act", and Republic Act No. 10173, otherwise known as the "Data Privacy Act of 2012", shall not apply to other financial accounts, which are subject of the investigation of BSP under this provision.

No bank or institution, or any of its directors, officers, or employees shall be subject to any action, claim, or demand in connection with, and shall be held free and harmless from liability for, any act done in compliance with an order for inquiry or examination of or other financial accounts from BSP: *Provided, furthermore,* That the BSP may use any or all information gathered from the above inquiry, examination, or investigation, in the course of its implementation of relevant provisions of Republic Act No. 11765 or the "Financial Products and Services Consumer Protection Act of 2022".

It shall be unlawful, however, for any official or employee, of a bank or institution or the BSP, to disclose any information concerning said other financial accounts to any person under such conditions other than in relation to the examination and investigation under this Section. It shall be unlawful for any person to use this Act

for persecution or harassment or as an instrument to hamper competition in trade and commerce.

The BSP shall have the authority to issue rules on the information sharing and disclosure with law enforcement and other competent authorities in connection with its examination and investigation of financial, e-wallets, and other financial accounts under this provision: *Provided, finally,* That any information which may be shared by BSP under this provision shall be used solely for the investigation and prosecution of cases involving the prohibited acts and other offenses defined under Section 4 and 5 of this Act.

Sec. 11. *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 situation 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. 12. *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. 13. *Implementing Rules and Regulations.* – Within sixty (60) days from the effectivity of this Act, the BSP in coordination with the Department of Justice, NBI, PNP, and the Department of Information and Communications Technology shall promulgate the necessary rules and regulations for the effective implementation of the provisions of this Act.

Sec. 14. *Congressional Oversight Committee*. – There is hereby created a Congressional Oversight Committee to monitor and oversee the implementation of the provisions of this Act. The Committee shall be composed of three (3) members from the Senate Committee on Banks, Financial Institutions and Currencies and three (3)

members from the House of Representatives Committee on Banks and Financial Intermediaries. The Chairpersons of the Senate and the House of Representatives committees shall be joint Chairpersons of this Oversight Committee. The two (2) other members from each House are to be designated by the Senate President and the Speak of the House of Representatives, respectively. The minority shall have at least one (1) representative from each Chamber.

Sec. 15. *Separability Clause*. – Should any provision herein be declared unconstitutional, the other provisions not affected shall remain in full force and effect.

Sec. 16. *Repealing Clause*. – All laws, decrees, orders, rules and regulations or other issuances or parts inconsistent with the provisions of this Act are hereby repealed, amended or modified accordingly.

Sec. 17. *Effectivity.* – This Act shall take effect fifteen (15) days after its publication in the *Official Gazette* or in at least two (2) national newspapers of general circulation.

Approved,