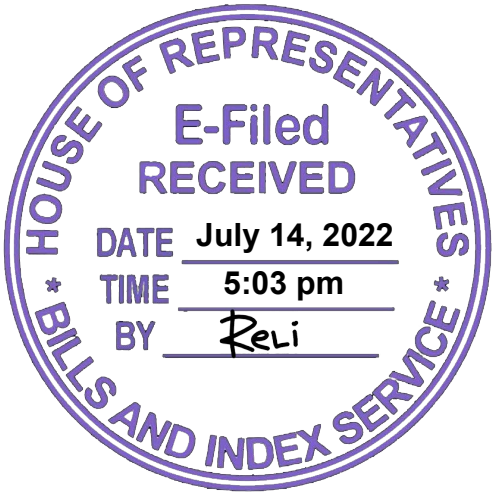
Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

NINETEENTH CONGRESS
First Regular Session

HOUSE BILL NO. 2013



Introduced by **HON. LUIS RAYMUND "LRAY" F. VILLAFUERTE, JR., HON. MIGUEL LUIS R. VILLAFUERTE, HON. TSUYOSHI ANTHONY G. HORIBATA AND HON. NICOLAS ENCISO VIII**

EXPLANATORY NOTE

Cybercrime has risen with the increase in the big shift in the way we live our lives and the use of the Internet. Unsurprisingly, criminals have taken advantage of the digitalization of banking, payment, and related systems. COVID-19 has presented several new opportunities for cybercriminal exploitation, including remote work, virtual crime, and persistent threats.

Banks have increased their efforts in addressing cybercrimes, and consumers are increasingly educated, vigilant and cautious with continuous use. The fact remains that the deterrence of cybercrimes needs supporting laws. At present, the Philippines does not have any law against the use of financial accounts as an accessory to a financial crime. No punishment can deter these criminal actions.

This proposed measure enumerates and defines punishable offenses such as money mules and phishing. Furthermore, due to the deleterious effect on the economy, the State declares that the commission of certain crimes under this proposed bill when done in bulk or on a large scale is a form of economic sabotage and a heinous crime and shall be punishable to the maximum level allowed by law. The recent gains in the digitalization of financial services should not result in adverse consequences.

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

LUIS RAYMUND "LRAY" F. VILLAFUERTE, JR.

MIGUEL LUIS R. VILLAFUERTE

TSUYOSHI ANTHONY G. HORIBATA

NICOLAS ENCISO VIII

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

NINETEENTH CONGRESS
First Regular Session

HOUSE BILL NO. 2013

Introduced by **HON. LUIS RAYMUND "LRAY" F. VILLAFUERTE, JR., HON. MIGUEL LUIS R. VILLAFUERTE, HON. TSUYOSHI ANTHONY G. HORIBATA AND HON. NICOLAS ENCISO VIII**

AN ACT
REGULATING THE USE OF BANK ACCOUNTS, ELECTRONIC WALLETS, AND OTHER FINANCIAL ACCOUNTS

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 *"Financial Accounts Regulation Act".*

SEC. 2. Declaration of Policy. – The State recognizes the vital role of banks, other 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 bank accounts and e-wallets or lure account holders into perpetrating fraudulent activities. It shall therefore be the policy of the State to regulate the use of bank accounts and e-wallets. Further, due to the deleterious 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 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 to a user's bank account or e-wallet;

b) ***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;

c) ***Bulk email or mass mailer*** refers to a service or software used to send electronic mail in mass or to fifty (50) or more emails;

d) ***Electronic Wallet or E-wallet*** refers to a digital value stored in either a software or application which the users can use for financial transactions such as payments, funds transfers, top-ups or cash in and/or withdrawals, among others. Example of e-wallets are e-money or virtual asset accounts stored in mobile or web-based apps;

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 committed the prohibited 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) ***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-for-profit;

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; and

i) ***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.

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. The following acts shall constitute an offense:

1. Opening a bank, e-wallet or other financial account and using or allowing the use thereof, to receive or transfer or withdraw proceeds derived from crimes, offenses, or social engineering schemes;
2. Opening a bank, e-wallet account 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;
3. Buying or renting a bank, e-wallet or other financial account for the purpose of receiving or transferring or withdrawing proceeds derived from crimes, offenses, or social engineering;
4. Selling a bank, e-wallet or other financial account for the purpose of receiving or transferring or withdrawing proceeds derived from crimes, offenses, or social engineering;
5. Account takeover or using or borrowing a bank or e-wallet account for the purpose of receiving or transferring or withdrawing proceeds derived from crimes, offenses, or social engineering; and
6. Recruiting, enlisting, contracting, hiring, utilizing or inducing any person to act as a money mule.

b) *Social engineering schemes*. Any person performing any social engineering schemes shall be penalized under this Act.

Social engineering scheme shall be deemed committed when a person performs any of the following:

1. Makes any communication to another person by representing one's self as a representative of a financial institution in order to gain the trust of others; and
2. Uses electronic communication to induce or request any person to provide sensitive identifying information with the intent to defraud or injure any person.

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 also constitute an offense:

(a) Any person who willfully abets or aids 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 the 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 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) hereof 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 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 constitute 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 (PhP100,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00) 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 power of representation of the juridical person: Provided, That the act committed falls within the scope of such authority; (b) an authority to make 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 (PhP10,000,000).

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 the *Bangko Sentral ng Pilipinas* (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 cybercrime units of the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) in the investigation of cases involving violations of this Act and in the enforcement and implementation of cybercrime warrants and related orders.

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 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. 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 (IRR). — Within sixty (60) days from the effectivity of this Act, the BSP, Department of Justice (DOJ), NBI, PNP, and the Department of Information and Communications Technology shall promulgate the rules and regulations to effectively implement the provisions of this Act.

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

SEC. 15. Separability Clause. If any section or provision of this Act shall be declared unconstitutional or invalid, the other sections or the provisions not affected thereby shall remain in full force and effect.

SEC. 16. Repealing Clause. All laws, decrees, executive orders, rules and regulations or parts thereof which are inconsistent with 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 a newspaper of general circulation.

Approved,