



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

EIGHTEENTH CONGRESS
Second Regular Session

House Bill No. 9615



Introduced by Representative Junie E. Cua
Lone District, Quirino

EXPLANATORY NOTE

The novel coronavirus pandemic accelerated the popularity of digital and “card-not-present” transactions which led banks to extend their reach and efficiency in the delivery of services to the public. As the banking industry continually implements its digitalization initiatives and enhances its cybersecurity systems, cybercriminals however continue to inflict harm by finding new and different ways to deceive the banks’ consumers. These cybercriminals have determined that retail customers are the “weak point” that can be exploited.

The economic hardship brought about by the pandemic has led some to resort to “easy money” or to look for funds obtained by dubious means or for little work, such as the buy-and-sell of bank accounts which phishers or cybercriminals use to avoid arrest and criminal liability.

This is why banks and consumers must join forces in addressing phishing and other cybercrime incidents to hold criminals accountable. While the banking industry continues to innovate its security systems to stop cybercriminals’ activities, consumers have equally a crucial part to play by being vigilant in knowing how they can defend themselves, and avoid participation and falling prey to the fraudulent mechanisms set-up by cybercriminals.

Any action undertaken to deter cybercriminals needs legislative support, given the fact that the Philippines, unlike places like Singapore, has no law against the use of financial accounts as accessories to financial crime—whether or not the accounts belong or are loaned to the fraudster. For the last three years, around 1,419 incidents were tied to deposit crimes and losses. The distinct lack of sufficient laws and penalties make it difficult to not only discourage cybercrime but also mete out disciplinary action. Collective action is necessary protect the financial industry and more importantly the banking public.

As such, we must take careful consideration of what can and should be done to mitigate the rise in cybercrime incidents. All legislation impacting digital financial services must be considered meticulously, so as not to reverse recent gains in digitalization of financial services, lest such legislation give rise to adverse economic consequences.

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

BAEWRA June 14, 2021
JUNIE E. CUA



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

EIGHTEENTH CONGRESS
Second Regular Session

House Bill No. 9615

Introduced by Representative Junie E. Cua
Lone District, Quirino

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:

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

3 **SECTION 2. *Declaration of Policy.*** – The State recognizes the vital role of both banks and
4 the general banking public in promoting and maintaining a stable and efficient financial system.
5 The State also acknowledges that in the advent of electronic commerce (e-commerce) and
6 digital banking, there is a need to protect the public from cybercriminals and criminal
7 syndicates who target bank accounts and e-wallets and lure account holders to aid them in
8 perpetrating fraudulent activities. It shall be the policy of the State to undertake measures to
9 protect all persons from falling prey to the various cybercrime schemes by regulating and
10 prohibiting the use of bank accounts and electronic wallets (e-wallets) for unusual and
11 suspicious financial activities. Furthermore, due to the deleterious effect on the economy, the
12 State declares that the commission of certain crimes under this Act when done in bulk or in
13 large scale is a form of economic sabotage and a heinous crime and shall be punishable to the
14 maximum level allowed by law.

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

17 (A) ***Account takeover*** refers to a form of identity theft and fraud, where a malicious third
18 party successfully gains access and control to a user's bank account or e-wallet.

- (B) **Bulk email/mass mailer** refers to a service or software used to send electronic mail (e-mail) in mass.
- (C) **Entity** refers to 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) **Money mule** refers to any person who electronically receives, acquires, or transfers money, funds, or proceeds derived from phishing or other cybercrime.
- (E) **Phishing** refers to a social engineering scheme to obtain or any attempt to obtain sensitive identifying information by disguising as a trusted entity in an electronic communication for the purpose of illegally accessing a victim's online account.
- (F) **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.
- (G) **Social engineering scheme** in the context of information security refers to the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. This includes phishing and any of its variations such as but not limited to vishing, smishing and other similar forms of deception.
- (H) **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 or amount involved is observed to deviate 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 committed, 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, phishing scheme or cybercrime
 5. any transaction that is similar, analogous or identical to any of the foregoing.
- (I) **Unusual activity** refers to the use of one's bank account or e-wallet that is not in accordance with the terms, conditions, and permitted purpose imposed by the bank or financial entity.

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

- (A) **Money mule.** It shall be prohibited for any person who, with intent to gain for himself or for another, electronically obtains, receives, acquires, or transfers money, funds, or proceeds derived from a suspicious activity, phishing or other cybercrime offense. Mere electronic receipt or transfer of money, funds, or proceeds which has been subject of a suspicious activity, phishing scheme or other cybercrime shall be prima facie evidence that the person is a money mule.

The following acts shall also constitute an offense:

- (1) Opening a bank or e-wallet account and using or allowing the use thereof, to receive or transfer 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 or transfer proceeds derived from a suspicious activity or cybercrime;
- (3) Buying or renting a bank or e-wallet account for the purpose of receiving or transferring proceeds derived from a suspicious activity or cybercrime;
- (4) Selling a bank or e-wallet account for the purpose of receiving or transferring 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 or transferring proceeds derived from a suspicious activity or cybercrime;
- (6) Recruiting, enlisting, contracting, hiring or inducing any person to electronically obtain, receive, acquire, or transfer 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.

Recruitment or utilization of money mules is deemed committed by a syndicate if carried out by a group of three (3) or more persons conspiring or confederating with one another. It is deemed committed in large scale if committed against three (3) or more persons individually or as a group.

(B) Phishing. It shall be prohibited for any person to obtain or attempt to obtain through a social engineering scheme, sensitive identifying information by disguising as a trusted entity in an electronic communication for the purpose of illegally accessing a victim's online account.

An individual or entity is guilty of phishing if, with intent to defraud or injure an individual or entity, or with knowledge that one is facilitating a fraud or injury to be perpetrated by anyone:

- (1) Makes any electronic communication disguising to be a trusted entity or on behalf of a trusted entity; and
- (2) Uses electronic communication to induce, request, or solicit any person to provide sensitive identifying information.

(C) Economic sabotage. Any offense perpetrated under this subsection using a bulk e-mail, mass mailer or any service, software, or other method of delivery calculated to utilize the massive reach of the internet to reach the maximum number of victims, pursuant to a "phishing" or other similar fraudulent scheme, shall be punished as an act of economic sabotage."

SECTION 5. Other Offenses. — The acts involving or having relation to the following shall also constitute an offense:

- 1 (a) Aiding or Abetting a Money Mule. — Any person who willfully abets or aids in the
2 commission of any of the offenses enumerated in this Act shall be held liable.
- 3 (b) Attempt in the commission of a crime. — Any person who willfully attempts to commit
4 any of the offenses enumerated in this Act shall be held liable.

5 **SECTION 6.** All crimes defined and penalized by the Revised Penal Code, as amended, and
6 special laws, if committed by, through and with the use of information and communications
7 technologies shall be covered by the relevant provisions of this Act: *Provided*, That the penalty
8 to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code,
9 as amended, and special laws, as the case may be.

10 **SECTION 7.** Liability under Other Laws. — A prosecution under this Act shall be without
11 prejudice to any liability for violation of any provision of the Revised Penal Code, as amended,
12 or special laws.

13 **SECTION 8. *Penalties.*** — Any person found guilty of the punishable act under Section 4(A)
14 shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred
15 thousand pesos (PhP200,000.00) but not exceeding Five hundred thousand pesos
16 (PhP500,000.00), or both.

17 Any person found guilty of any of the punishable acts enumerated in Section 4(B) shall be
18 punished with imprisonment of *prision correccional* or a fine of at least One hundred thousand
19 pesos (PhP100,000.00) but not exceeding Two hundred thousand pesos (PhP200,000.00), or
20 both.

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

24 Any person found guilty of any of the offenses that constitutes economic sabotage under Section
25 4(C) shall be punished with life imprisonment and a fine of not less than One million pesos
26 (P1,000,000.00) but not more than Five Million Pesos (P5,000,000.00).

27 **SECTION 9. *Implementing Rules and Regulations.*** — Within thirty (30) days from the
28 effectivity of this Act, the Bangko Sentral ng Pilipinas (BSP) Department of Justice (DOJ),
29 National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall
30 promulgate the rules and regulations to effectively implement the provisions of this Act.

31 **SECTION 10. *Jurisdiction.*** — The Regional Trial Court shall have jurisdiction over any
32 violation of the provisions of this Act including any violation committed by a Filipino national
33 regardless of the place of commission. Jurisdiction shall lie if any of the elements was
34 committed within the Philippines or committed with the use of any computer system wholly or
35 partly situated in the country, or when by such commission any damage is caused to a natural
36 or juridical person who, at the time the offense was committed, was in the Philippines.

37 **SECTION 11. *General Principles Relating to International Cooperation.*** — All relevant
38 international instruments on international cooperation in criminal matters, arrangements agreed
39 on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent
40 possible for the purposes of investigations or proceedings concerning criminal offenses related
41 to computer systems and data, or for the collection of evidence in electronic form of a criminal,
42 offense shall be given full force and effect.

1 **SECTION 12. *Separability Clause.*** If any separable provision of this Act is declared
2 unconstitutional, the remaining provisions shall continue to be in force.

3 **SECTION 13. *Repealing Clause.*** All laws, decrees, executive orders, rules and regulations or
4 parts thereof which are inconsistent with this Act are hereby repealed, amended or modified
5 accordingly.

6 **SECTION 14. *Effectivity.*** This Act shall take effect fifteen (15) days after its publication in
7 the *Official Gazette* or in a newspaper of general circulation.