



Senate
Office of the Secretary

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

23 MAR 22 P4:57

**SENATE
S.B. No. 2039**

RECEIVED BY: _____

Introduced by Senator Juan Miguel F. Zubiri

**AN ACT
PROHIBITING MONEY MULES AND OTHER FRAUDULENT ACTS INVOLVING
BANK ACCOUNTS, E-WALLETS, AND OTHER FINANCIAL ACCOUNTS,
PROVIDING PENALTIES THEREFOR AND FOR OTHER PURPOSES**

EXPLANATORY NOTE

The use of digital banking and online financial transactions has accelerated amid the COVID-19 global pandemic, allowing millions of Filipinos to perform banking tasks without going outside of their homes. Based on a report by the Philippine Daily Inquirer, as of February 2022, 70 percent of the Philippines' adult population are online banking users. The convenience and accessibility of online banking, coupled with the promise of security made by various digital banking platforms, led to an increase in users over the past few years.

However, fraudulent financial activities are on the rise as the world adjusts to fast-paced technological advancements in digital banking and e-commerce in the financial sector. The Bangko Sentral ng Pilipinas (BSP) received 42,456 complaints between 2020 and 2021 related to digital financial fraud and called for its regulated financial institutions to take steps in preventing cyber attacks in the financial sector.

As reliance on digital transactions grows, the times call for the augmented protection of millions of users from money mules and other fraudulent schemes involving bank accounts, e-wallets, and other financial accounts.

This bill prohibits money mules and other fraudulent financial activities in order to protect Filipinos from becoming victims of such schemes. It aims to declare certain activities defined herein as a form of economic sabotage and a heinous crime and seeks to penalize persons found guilty of committing financial fraud as defined by its provisions.

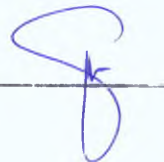
In view of the foregoing, the passage of this bill is earnestly sought.

JUAN MIGUEL F. ZUBIRI

23 MAR 22 P4 57

SENATE

RECEIVED BY: _____



S.B. No. 2039

Introduced by Senator Juan Miguel Zubiri

AN ACT

PROHIBITING MONEY MULES AND OTHER FRAUDULENT ACTS INVOLVING BANK ACCOUNTS, E-WALLETS, AND OTHER FINANCIAL ACCOUNTS, PROVIDING PENALTIES THEREFOR AND FOR OTHER PURPOSES

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

1 **Section 1. Short Title.** – This Act shall be known as the “Anti-Money Mule and
2 Financial Fraud Act of 2023.”

3

4 **Sec. 2. Declaration of Policy.** – The State recognizes that with the advent of
5 digital banking and finance and electronic commerce (e-commerce), there is a need to
6 protect the public from cybercriminals and criminal syndicates who target bank accounts,
7 electronic wallets (e-wallets), or other financial accounts or lure account holders into
8 perpetrating or aiding fraudulent activities. It shall therefore be the policy of the State to
9 undertake measures to protect all persons from falling prey to the various fraudulent
10 schemes by regulating the use of bank accounts, e-wallets, and other financial accounts,
11 and preventing their use in fraudulent activities. Furthermore, due to the deleterious effect
12 on the economy, the large-scale commission of certain crimes under this Act is hereby
13 declared a form of economic sabotage and a heinous crime and shall be severely punished.

14

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

- 17 a. *Account Takeover* is committed by a person who by any means, such as but not
18 limited to force, intimidation, manipulation, or deceit, gains access and control of
19 an account owner’s bank account, e-wallet, or other financial account;
- 20 b. *Account owner* refers to the owner/s of a bank account, e-wallet or other financial
21 account, as registered with the bank or financial institution;
- 22 c. *Bank Account* refers to an interest or non-interest bearing deposit, trust,
23 investment and other transaction account maintained with a bank or a financial
24 institution;

- 1 d. *Bulk or Mass Messaging* refers to the act of sending messages by means of
2 electronic mail (email), short messaging service (SMS), chat message, or other
3 written, digital or electronic form of communication to an aggregate or total of
4 thirty (30) recipients or more, counted from the first to the last act of sending;
5 e. *Electronic Wallet (e-wallet)* refers to a transaction account which stores monetary
6 value through an electronic instrument or device, which is pre-funded to enable
7 the processing of financial transactions, including but not limited to payments or
8 fund transfers to other individuals or entities. Examples of e-wallets include
9 electronic money or virtual asset accounts stored in mobile phones or web-based
10 apps.
11 f. *Money Mule* refers to any person who obtains, receives, acquires, transfers,
12 withdraws or otherwise transacts with money, funds, virtual assets, property or
13 proceeds derived from crimes, offenses or social engineering schemes, on behalf
14 or for the benefit of another person, including the perpetrators of the crime,
15 offense, or social engineering scheme, as punished under Section 4(a) of this Act;

16 For this purpose, money, funds, property or proceeds shall include but not be
17 limited to coins or currency of legal tender of the Philippines or another jurisdiction,
18 electronic money, virtual assets, securities or negotiable instruments, other
19 monetary or financial instruments, or all things which are or may be the object of
20 appropriation.

- 21 g. *Other Financial Accounts* refer to new or emerging forms of financial accounts
22 other than bank accounts and e-wallets;
23 h. *Phishing* refers to a social engineering scheme whereby a person falsely represents
24 himself or herself to another person as a legitimate institution, entity or person or
25 as a representative thereof, for the purpose of obtaining the latter's sensitive
26 identifying information and/or accessing and transacting the latter's bank, e-wallet,
27 or other financial account;
28 i. *Sensitive Identifying Information* refers to any information that can be used to
29 access as bank, e-wallet, or other financial accounts such as, but not limited to,
30 usernames, passwords, bank account details, credit card, debit card, Personal
31 Identification Number (PIN), among other electronic information or credentials;
32 j. *Social Engineering Scheme* refers to the use of deception or other fraudulent
33 means to obtain confidential or personal information, including sensitive identifying
34 information, of another individual or entity.

35 Social engineering schemes may be committed in-person or through various media
36 or platforms, including but not limited to:

- 37 1. Electronic mail;
- 38 2. Short Message Service, text messages, or other message services;
- 39 3. Social media sites;
- 40 4. Websites;
- 41 5. Telephone or voice calls;
- 42 6. Mobile or other electronic applications;
- 43 7. Advertisements; or
- 44 8. Search engines.

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

3 a. *Money mule.* It shall be prohibited for any person to act as a money mule or
4 engage another person to act as a money mule, as defined below. The following
5 acts shall be punishable under this Act:

6
7 1. The registration or opening of a bank account, e-wallet or other financial
8 account with the use of a fictitious name or identity, falsified or
9 tampered identification documents, or by using the identity or
10 identification documents of another person;

11 2. The sale or transfer of a bank account, e-wallet or other financial
12 account to any person who is not its registered account owner, or
13 otherwise allowing the use of a bank account, e-wallet or other financial
14 account by persons who are not its registered owner: *Provided*, That the
15 offense hereunder may be committed by the account owner or any
16 person who holds or possesses an account registered in the name of
17 another person; *Provided further*, That if the sale, transfer, or allowing
18 of others to use the account is knowingly made to aid other persons to
19 commit an unlawful activity or to receive, withdraw or otherwise transact
20 with money or property constituting proceeds derived from an unlawful
21 activity, the penalty to be imposed shall be one (1) degree higher.

22 3. The purchase, use, borrowing or possession by a person who is not an
23 account owner of another person’s bank account, e-wallet or other
24 financial account: *Provided*, That if the purchase, use, borrowing or
25 possession by a person is made for the purpose of committing an
26 unlawful activity or for receiving, withdrawing, or otherwise transacting
27 with money or property constituting proceeds from an unlawful activity,
28 the penalty to be imposed shall be one (1) degree higher; Recruiting,
29 enlisting, contracting, hiring or inducing any person to register a bank
30 account, e-wallet or other financial account for the purpose of later
31 transferring or ceding control or possession of the same to any other
32 person who is not the registered account owner; *Provided further*, That
33 if the person being recruited, enlisted, contracted, hired, or induced to
34 open or register an account is a minor below 18 years old or senior
35 citizen aged 60 years old or above, the penalty to be imposed shall be
36 one (1) degree higher;

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

44
45 c. *Account takeover.* A person shall be prohibited from committing account
46 takeover, as defined under Section 3 (a) of this Act;

47

1 d. *Economic Sabotage.* Any offense defined under this Section shall be considered
2 as an offense involving economic sabotage when any of the following
3 circumstances is present:

- 4 1. The offense was committed by a syndicate;
- 5 2. The offense was committed in large scale; or
- 6 3. The individual or aggregate amount involved in the offense is greater
7 than Two Million Pesos (PhP2,000,000.00).

8
9 For this purpose, an act shall be deemed committed by a syndicate if the offense
10 was carried out by a group of three (3) or more persons conspiring or confederating with
11 one another, while an act shall be deemed committed in large scale if the offense was
12 committed against three (3) or more persons individually or as a group.

13
14 **Sec. 5. Other Offenses.** – The following shall also constitute an offense:

- 15 a. *Aiding or Abetting.* Any person who willfully abets or aids in the commission of any
16 of the offenses enumerated under Section 4 of this Act shall be held liable; and
- 17 b. *Attempt in the Commission of an Offense.* Any person who attempts to commit
18 any of the offenses enumerated under Section 4 of this Act shall be held liable.

19
20 **Sec. 6. Liability Under Other Laws.** – A prosecution under this Act shall be
21 without prejudice to any liability for violation of any provision of the Revised Penal Code,
22 as amended, or special laws, including but not limited to Republic Act Nos. 8484, 9160,
23 and 10175, as amended.

24
25 **Sec. 7. Penalties.** – Any person found guilty of the punishable act under Section
26 4 (a) shall be punished with imprisonment of *prision mayor in its minimum period* and a
27 fine of at least One Hundred Thousand Pesos (P100,000.00) but not exceeding Two
28 Hundred Thousand Pesos (P200,000.00), or both.

29 Any person found guilty of any of the punishable acts enumerated in Section 4 (b)
30 and (c) shall be punished with imprisonment of *prision mayor in its maximum period* and
31 a fine of at least Two Hundred Thousand Pesos (P200,000.00) but not exceeding Five
32 Hundred Thousand Pesos (P500,000.00), or both: *Provided*, That the maximum penalty
33 shall be imposed if the target or victim of the social engineering scheme is or includes a
34 senior citizen aged sixty (60) years old or above at the time the offense was committed or
35 attempted.

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

39 Any person found guilty of any of the punishable acts enumerated in Section 5 shall
40 be punished with imprisonment one (1) degree lower than that of the prescribed penalty
41 for the offense or a fine of at least One Hundred Thousand Pesos (P100,000.00) but not
42 exceeding Five Hundred Thousand Pesos (P500,000.00) or both.

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

8

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

15

16 **Sec. 10. Enforcement.** – The National Bureau of Investigation (NBI) and Philippine
17 National Police (PNP) shall be responsible for the efficient and effective law enforcement
18 of the provisions of this Act. The cybercrime unit or center established under Section 10 of
19 Republic Act No. 10175 shall exclusively handle all cases involving violations of this Act:
20 *Provided,* That they shall coordinate closely with the *Bangko Sentral ng Pilipinas* and other
21 relevant government agencies in the investigation and enforcement of cybercrime warrants
22 and related orders.

23

24 **Sec. 11. Duties of Banks and Financial Institutions.** – Banks, Non-Bank Financial
25 Institutions, and other pertinent Bank and Non-Bank Institutions shall respond to all
26 consumer complaints related to phishing, social engineering schemes, account takeover or
27 other cybercrimes that are committed on their platform. They shall investigate each case,
28 exert reasonable efforts to assist victims recover their direct monetary loss, if any, and
29 provide evidence in support of any criminal investigations or legal actions that may be
30 initiated by the victims or legal authorities.

31

32 The said institutions shall likewise institute measures to strengthen their online platforms,
33 payment systems, and data security to prevent fraud.

34

35 **Sec. 12. Implementing Rules and Regulations.** – Within sixty (60) days from
36 the effectivity of this Act, the *Bangko Sentral ng Pilipinas* (BSP), Department of Justice
37 (DOJ), Department of Information and Communications Technology (DICT), NBI and PNP
38 shall jointly promulgate the rules and regulations to effectively implement the provisions of
39 this Act.

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

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

5

6 **Sec. 13. *Appropriation.*** – The amount necessary for the effective implementation
7 of this Act shall be incorporated in the General Appropriations Act.

8

9 **Sec. 14. *Separability Clause.*** – If for any reason, any provision of this Act is
10 declared invalid or unconstitutional, the remaining parts or provisions not affected shall
11 remain in full force and effect.

12

13 **Sec. 15. *Repealing Clause.*** – All laws, decrees, executive orders, rules and
14 regulations or parts thereof which are contrary or inconsistent with the provisions of this
15 Act are hereby repealed, amended or modified accordingly.

16

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

Approved,