



HOUSE OF REPRESENTATIVES

H. No. 7393

BY REPRESENTATIVES TIENG, VILLAFUERTE (L.R.), VILLAFUERTE (M.L.), HORIBATA, ENCISO, RODRIGUEZ (E.), ESPARES, TARRIELA, FARIÑAS, CASTRO (F.), SALCEDA, BONGALON, CUA, DALIPE, MARCOS, LACSON-NOEL, PRIMICIAS-AGABAS, BOLILIA, PUMAREN, ACIDRE, BARONDA, DELOS SANTOS, VELOSO-TUAZON, OAMINAL, DY (F.), ORTEGA, ADVINCULA, KHONGHUN, PANALIGAN, SANTOS, SUANSING (M.A.), TEODORO, NOGRALES (M.), REVILLA (B.), ZAMORA (Y.M.), DOMINGO, ARBISON, VARGAS, ROQUE, ZAMORA (A.M.), ESCUDERO, TAN (K.M.), ACHARON, FORTES, SAULOG, LIBANAN, DAZA, HERRERA, ABALOS, MADRONA, ALVAREZ (M.), GO (M.), UNABIA, OLIVAREZ, ALVAREZ (J.), RODRIGUEZ (R.), NAVA, DIMAPORO (M.K.), TANJUATCO, YAMSUAN AND TUTOR, PER COMMITTEE REPORT NO. 376

AN ACT
REGULATING THE USE OF FINANCIAL ACCOUNTS

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-Financial*
2 *Account Scamming Act*”.
- 3 **SEC. 2. Declaration of Policy.** – The State recognizes the vital role of banks, other
4 payment service providers, and the general banking public in promoting and
5 maintaining a stable and efficient financial system. The State also acknowledges
6 that with the increased use of electronic commerce and digital banking, there is a
7 need to protect the public from cybercriminals and criminal syndicates who target
8 financial accounts, e-wallets, and other financial accounts, or lure account holders
9 into perpetrating fraudulent activities. It shall therefore be the policy of the State to
10 regulate the use of financial accounts, e-wallets, and other financial accounts.

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

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

- 5 (a) **Account takeover** refers to a form of identity theft and fraud, where a
6 malicious third party successfully gains access and control over a user's
7 financial account, e-wallet, or other financial account;
- 8 (b) **Bulk email or mass mailer** refers to a service or software used to send
9 electronic mail in mass or to fifty (50) or more emails;
- 10 (c) **Electronic Wallet or E-wallet** refers to a digital value stored in a wallet as
11 may be defined by the *Bangko Sentral ng Pilipinas* (BSP) regulations;
- 12 (d) **Financial Account** refers to an interest or non-interest bearing deposit,
13 trust, investment, credit card, and other transaction account maintained with
14 a bank, non-bank, or financial institution;
- 15 (e) **Money mule** refers to any person who obtains, receives, acquires, or
16 transfers or withdraws money, funds, or proceeds derived from crimes,
17 offenses, or social engineering schemes, and those who commit the
18 prohibited acts under Section 4(a) of this Act;
- 19 (f) **Multi-Factor Authentication (MFA)** refers to an authentication method
20 that requires the user to provide two (2) or more verification factors, such
21 as something you know, something you have, and something you are, to
22 gain access to a resource;
- 23 (g) **Other Financial Accounts** refer to the various types of accounts used for
24 financial transactions other than financial accounts and e-wallets;
- 25 (h) **Persons** refer to natural or juridical persons, including corporations,
26 partnerships, associations, organizations, joint ventures, government
27 agencies or instrumentalities, government-owned and controlled
28 corporations (GOCCs), or any other legal entity, whether for profit or
29 not-for-profit;
- 30 (i) **Sensitive Identifying Information** refers to any information that can be
31 used to access an individual's financial accounts such as, usernames,
32 passwords, bank account details, credit card, debit card, and e-wallet
33 information among other electronic credentials; and
- 34 (j) **Social engineering scheme** refers to the use of deception or fraudulent
35 means by a person to obtain confidential or personal information, including

1 sensitive identifying information, of another person, and those acts
2 enumerated under Section 4(b) of this Act.

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

5 (a) *Money mule.* It shall be prohibited for any person to act as a money mule.
6

7 Any person performing any of the following acts shall be considered as a
8 money mule:
9

10 (1) Opening a financial, e-wallet, or other financial account and
11 using or allowing the use thereof, to receive or transfer or
12 withdraw proceeds known to be derived from crimes, offenses,
13 or social engineering schemes;
14

15 (2) Opening a financial, e-wallet, or other financial account under a
16 fictitious name or using the identity or identification documents
17 of another to receive or transfer or withdraw proceeds derived
18 from crimes, offenses, or social engineering schemes;
19

20 (3) Buying or renting a financial, e-wallet, or other financial
21 account for the purpose of receiving or transferring or
22 withdrawing proceeds derived from crimes, offenses, or social
23 engineering schemes;
24

25 (4) Selling and lending a financial, e-wallet, or other financial
26 account for the purpose of receiving or transferring or
27 withdrawing proceeds derived from crimes, offenses, or social
28 engineering schemes;
29

30 (5) Performing account takeover or using or borrowing a financial,
31 e-wallet, or other financial account for the purpose of receiving
32 or transferring or withdrawing proceeds derived from crimes,
33 offenses, or social engineering schemes; or

1 (6) Recruiting, enlisting, contracting, hiring, utilizing or inducing
2 any person to perform the acts mentioned in items 1 to 5 of this
3 Section.
4

5 (b) *Social engineering schemes.* Any person performing any social engineering
6 scheme shall be penalized under this Act.
7

8 Social engineering scheme shall also be deemed committed when a
9 person performs any of the following:
10

11 (1) Makes any communication to another person by representing
12 one's self as a representative of a financial institution or making
13 any false representation in order to gain the trust of others and
14 solicit sensitive identifying information that results in account
15 takeover; or
16

17 (2) Uses electronic communication to induce or request any person
18 to provide sensitive identifying information with the intent to
19 defraud or injure any person.
20

21 Banks and other financial institutions shall ensure that access to their
22 clients' accounts are protected by layers of security, including, but not
23 limited to, multi-factor authentication (MFA), and other account-holder
24 authentication and verification processes: *Provided*, That, such security
25 levels are proportionate and commensurate to the nature, size and
26 complexity of their operations. Subject to sufficient and undeniable proof
27 resulting from a thorough investigation within a reasonable time, failure of
28 these institutions to exercise proper diligence shall result to immediate
29 restitution of amounts lost to the rightful owners.
30

31 (c) *Economic sabotage.* Any offense defined under this Section shall be
32 considered as an offense involving economic sabotage when any of the
33 following circumstances are present:

- 34 (1) The offense was committed by a syndicate;
35 (2) The offense was committed in large scale; or
36 (3) The offense was committed using a mass mailer.

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

6 **SEC. 5. *Other Offenses.*** – The acts involving or having relation to the following
7 shall also constitute an offense:

8 (a) Any person who willfully abets or aids in the commission of any of the
9 offenses enumerated in Section 4 of this Act shall be held liable; and

10
11 (b) Any person who willfully attempts to commit any of the offenses
12 enumerated in Section 4 of this Act shall be held liable.

13 **SEC. 6. *Higher Penalty for Acts Committed Under the Revised Penal Code and***
14 ***Crimes Under Special Laws Using Money Mule and Social Engineering***
15 ***Schemes.*** – All crimes defined and penalized by Act No. 3815, otherwise known
16 as the Revised Penal Code, as amended, and special laws, if committed by and
17 through the acts as defined under Section 4 hereof, shall be covered by the relevant
18 provisions of this Act: *Provided*, That the penalty to be imposed shall be one (1)
19 degree higher than that provided for by the Revised Penal Code, as amended, and
20 special laws, as the case may be.

21 **SEC. 7. *Liability Under Other Laws.*** – A prosecution under this Act shall be
22 without prejudice to any liability for violation of any provision of the Revised
23 Penal Code, as amended, or special laws.

24 **SEC. 8. *Penalties.*** – Any person found guilty of the punishable act under
25 Section 4(a) hereof shall be punished with imprisonment of *prision correccional* or
26 a fine of at least One hundred thousand pesos (PhP100,000.00) but not exceeding
27 Two hundred thousand pesos (PhP200,000.00), or both.

28 Any person found guilty of any of the punishable acts enumerated in Section 4(b)
29 hereof shall be punished with imprisonment of *prision mayor* or a fine of at least
30 Two hundred thousand pesos (PhP200,000.00) but not exceeding Five hundred
31 thousand pesos (PhP500,000.00), or both: *Provided, however*, That the maximum
32 penalty shall be imposed if the target or victim of the social engineering scheme is
33 or includes a senior citizen aged sixty (60) years old or above at the time the
34 offense was committed or attempted.

1 Any person found guilty of any of the offenses that constitutes economic sabotage
2 under Section 4(c) hereof shall be punished with life imprisonment and a fine of
3 not less than One million pesos (P1,000,000.00) but not more than Five million
4 pesos (P5,000,000.00).

5 Any person found guilty of any of the punishable acts enumerated in Section 5
6 hereof shall be punished with imprisonment one (1) degree lower than that of the
7 prescribed penalty for the offense or a fine of at least One hundred thousand pesos
8 (PhP100,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00),
9 or both.

10 **SEC. 9. Corporate Liability.** – When any of the punishable acts herein defined
11 knowingly committed on behalf of or for the benefit of a juridical person, by a
12 natural person who has a leading position within based on (a) a power of
13 representation of the juridical person: *Provided*, That the act committed falls
14 within the scope of such authority; (b) an authority to take decisions on behalf of
15 the juridical person: *Provided*, That the act committed falls within the scope of
16 such authority; or (c) an authority to exercise control within the juridical person,
17 the juridical person shall be held liable for a fine equivalent to at least double the
18 fines imposable in Section 8 hereof up to a maximum of Ten million pesos
19 (PhP10,000,000).

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

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

1 financial accounts, e-wallets, and other financial accounts, which are subject of the
2 investigation of BSP under this provision.

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

11 It shall be unlawful, however, for any official or employee, of a bank or institution
12 or the BSP, to disclose any information concerning said other financial accounts to
13 any person under such conditions other than in relation to the examination and
14 investigation under this Section. It shall be unlawful for any person to use this Act
15 for persecution or harassment or as an instrument to hamper competition in trade
16 and commerce.

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

24 **SEC. 11. *Jurisdiction.*** – The Regional Trial Court designated as cybercrime
25 court shall have jurisdiction over any violation of the provisions of this Act
26 including any violation committed by a Filipino national regardless of the place of
27 commission. Jurisdiction shall lie if any of the elements was committed within the
28 Philippines or committed with the use of any computer system wholly or partly
29 situated in the country, or when by such commission any damage is caused to a
30 natural or juridical person who, at the time the offense was committed, was in the
31 Philippines.

32 **SEC. 12. *General Principles Relating to International Cooperation.*** – All
33 relevant international instruments on international cooperation in criminal matters,
34 arrangements agreed on the basis of uniform or reciprocal legislation, and domestic
35 laws, to the widest extent possible for the purposes of investigations or proceedings
36 concerning criminal offenses related to computer systems and data, or for the

1 collection of evidence in electronic form of a criminal offense, shall be given full
2 force and effect.

3 **SEC. 13. *Implementing Rules and Regulations (IRR).*** – Within sixty (60) days
4 from the effectivity of this Act, the BSP, in coordination with the Department of
5 Justice (DOJ), NBI, PNP, and the Department of Information and Communications
6 Technology (DICT), shall promulgate the rules and regulations to effectively
7 implement the provisions of this Act.

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

12 **SEC. 14. *Congressional Oversight Committee.*** – There is hereby created a
13 Congressional Oversight Committee to monitor and oversee the implementation of
14 the provisions of this Act. The Committee shall be composed of three (3) members
15 from the Senate Committee on Banks, Financial Institutions and Currencies and
16 three (3) members from the House of Representatives Committee on Banks and
17 Financial Intermediaries. The Chairpersons of both the Senate and the House of
18 Representatives committees shall be joint Chairpersons of this Committee. The two
19 (2) other members from each House are to be designated by the Senate President
20 and the Speaker of the House of Representatives, respectively. The minority shall
21 have at least one (1) representative from each Chamber.

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

25 **SEC. 16. *Repealing Clause.*** – All laws, decrees, executive orders, rules and
26 regulations or parts thereof which are inconsistent with this Act are hereby
27 repealed, amended or modified accordingly.

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

Approved,