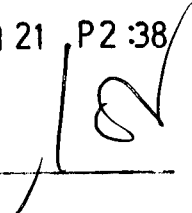


NINETEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
Second Regular Session)

24 FEB 21 P2 :38

RECEIVED BY: _____



SENATE

S. No. 2560

(In Substitution of S.B. Nos. 336, 1663, 2039, 2171, 2306 and 2407, taking into consideration H.B. No. 7393)

Prepared by the Committee on Banks, Financial Institutions & Currencies, with Senators Poe, Marcos, Zubiri, Estrada, Villanueva, Gatchalian, Legarda, Revilla and Villar M., as authors thereof

An Act Prohibiting Money Mules and Other Fraudulent Acts Involving Bank Accounts, E-Wallets, and Other Financial Accounts, and Providing Penalties Therefor

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 Account
2 Scamming Act (AFASA)".

3 **SEC. 2. Declaration of Policy.** - The State recognizes the vital role of banks, non-
4 banks, financial institutions, and other financial and payment service providers, and
5 the general banking public in promoting and maintaining a stable and efficient financial
6 system. The State also acknowledges that with the increased use of electronic
7 commerce and digital financial services, there is a need to promote awareness on the
8 proper use of financial accounts and to protect the public from cybercriminals and
9 criminal syndicates who target financial accounts or lure account holders into
10 becoming accessory and/or perpetrating fraudulent activities. It shall therefore be the
11 policy of the State to undertake measures to protect all persons from falling prey to
12 the various cybercrime schemes by regulating the use of financial accounts, and
13 preventing their use in fraudulent activities.

1 Further, due to the deleterious effect on the economy, the large-scale commission of
2 certain crimes under this Act shall be 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, the following terms are hereby
5 defined as follows:

- 6 a) **Account takeover** refers to an instance when a person gains access and
7 control over another person's financial account;
- 8 b) **Account owner** refers to the owner or owners of a financial account, such as
9 but not limited to bank accounts or e-wallets, opened, maintained, or registered
10 with a Responsible Institution;
- 11 c) **Electronic Communications** refer to digital platforms used to send and
12 receive messages or information, such as but not limited to: phone calls, SMS
13 or text messages, emails, social media platforms, electronic mail, other instant
14 messaging technologies, or websites;
- 15 d) **Electronic Wallet or E-wallet** refers to a store of value or electronic
16 instrument or device, which contain digital value as may be defined by the
17 Bangko Sentral ng Pilipinas (BSP) regulations;
- 18 e) **Financial Account** refers to any of the following:
19 1. An interest or non-interest-bearing deposit, trust investment, credit
20 card account; or
21 2. Other transaction account maintained with a bank, non-bank, or
22 financial institution; or
23 3. E-wallet; or
24 4. Virtual assets accounts; or
25 5. Any other type of digital account used for financial accounts, other
26 than bank accounts, e-wallets, and virtual assets accounts; or
27 6. Any other account used to avail financial products or services defined
28 under Section 3(c) of Republic Act No. 11765 or the Financial
29 Products and Services Consumer Protection Act;
- 30 f) **Fraud Management Systems (FMS)** refers to a comprehensive set of
31 automated and real-time monitoring and detection systems to identify and
32 block suspicious or fraudulent online transactions;
- 33 g) **Mass Mailer** refers to a service or software used to send electronic messages,
34 short messaging service (SMS), or electronic mail (email), or other written,
35 digital or electronic form of communication in mass to an aggregate of fifty (50)
36 recipients or more;
- 37 h) **Money Mule** - refers to any person who commits any of the acts under Section
38 4 (a) hereof;
- 39 i) **Multi-Factor Authentication (MFA)** refers to an authentication method that
40 requires two (2) or more verification factors to gain access to a resource;
- 41 j) **Responsible Institutions** refers to banks, non-banks, other financial
42 institutions, payments and financial service providers that are under the

1 jurisdiction of the BSP, and such other institutions as may be determined by
2 the BSP;

3 k) **Financial Account Information** refers to any information that can be used
4 as account identifier to access an individual's financial accounts such as, but
5 not limited to, usernames, passwords, bank account details, credit card, debit
6 card, and e-wallet information, among other electronic credentials;

7 l) **Social engineering scheme** refers to the use of deception, misrepresentation
8 or other fraudulent means by a person to obtain confidential or personal
9 information, including the financial account information of another person and
10 those acts enumerated under Section 4(b) of 2 this Act;

11 **SEC. 4. Prohibited Acts.** - The following acts shall constitute an offense punishable
12 under this Act:

13 a. *Money mule.* Any person who obtains, receives, acquires, keeps or transfers or
14 withdraws money, funds, or proceeds known or ought to be known through
15 ordinary diligence that the funds or proceeds are derived from crimes, offenses, or
16 social engineering schemes, or those who perform any of the following acts shall
17 be considered as a money mule:

18 1. Opening, using or allowing the use of a financial account in order to deposit,
19 receive, keep, transfer, or withdraw funds or proceeds known or ought to be
20 known through ordinary diligence that the funds or proceeds are derived from
21 crimes, offenses, or social engineering schemes; or

22 2. Opening a financial account under a fictitious name or using the identity or
23 identification documents of another person or other falsified documents; or

24 3. Buying, or renting another person's financial account, regardless of the
25 account owner's knowledge or consent to deposit, receive, keep, transfer, or
26 withdraw funds or proceeds known or ought to be known through ordinary
27 diligence that the funds or proceeds are derived from crimes, offenses, or social
28 engineering schemes;

29 4. Selling one's own financial account in order to deposit, receive, keep,
30 transfer, or withdraw funds or proceeds known or ought to be known through
31 ordinary diligence that the funds or proceeds are derived from crimes, offenses,
32 or social engineering schemes: *Provided, That,* if the seller has established by
33 clear and convincing evidence that he has no knowledge or participation as to
34 the manner the financial account he sold is to be utilized, the penalty to be
35 imposed for his act of selling his own financial account shall be the same penalty
36 imposed for violations of Section 5 of this Act;

37 5. Borrowing, or using another person's a financial account regardless of the
38 account owner's knowledge or consent, to deposit, receive, transfer, or
39 withdraw funds or proceeds, known or ought to be known by ordinary diligence
40 that the funds or proceeds are derived from crimes, offenses, or social
41 engineering schemes; or

1 6. Recruiting, enlisting, contracting, hiring, utilizing, or inducing any person to
2 be a money mule or to perform any of the acts mentioned in items 1 to 5 of
3 this Section.

4 *b. Social Engineering Schemes.* Any person performing any social engineering
5 scheme shall be penalized under this act. Social engineering shall be deemed
6 committed when a person performs any of the following:

7 1. Makes any communication to another person by misrepresenting oneself as
8 a representative of a Responsible Institution, or making any false
9 representation to solicit financial account information that may result, or
10 resulted to account takeover; or
11

12 2. Uses electronic means, tools, communication, or any other applicable
13 communication technology, or those similar thereto, such as, but not limited to,
14 social media platforms, electronic mails, or websites, to induce or request any
15 person to provide financial account information that may result, or resulted to
16 loss, damage or injury to any person.

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

20 1. The offense was committed by a syndicate; or

21 2. The offense was committed in large scale; or

22 3. The offense was committed using a mass mailer or other similar tools used
23 to send bulk emails or SMS, generative artificial intelligence or any similar
24 technology that takes advantage of the reach, open access and processing
25 power available through the internet to (a) collect and process large amounts
26 of data, (b) break secure passwords and encrypted data, (c) replicate likeness
27 and voices of natural persons, (d) create fake identities, likenesses, and voices,
28 or (e) other analogous uses that apply new technology to cause widespread
29 damage to the public;

30 4. The offense was committed by a group of foreign nationals operating inside
31 or outside the Philippines; or

32 5. The offense was committed through human trafficking.

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

38 **SEC. 5. Other Offenses.** - The following acts, or any acts involving or having relation
39 thereto shall also constitute as punishable offenses:

1 a) Willfully abetting or aiding in the commission of any of the offenses enumerated
2 under Section 4 of this Act;

3 b) Attempting to commit any of the offenses enumerated under Section 4 of this
4 Act;

5 c) Illegally obtaining any information related to financial accounts through
6 unauthorized means or through violation of any laws on data privacy and
7 cybersecurity;

8 d) Using any information from financial accounts to intimidate, unduly harass the
9 account owner or threaten the use financial account of the account owner for
10 unlawful means to derive a monetary benefit or any other benefit of whatever
11 form or nature from the account owner;

12 **SEC. 6. Responsibility to Protect Access to Financial Accounts.-** Responsible
13 Institutions shall ensure that access to their clients' financial accounts are protected
14 by adequate risk management systems and controls including, but not limited to,
15 multi-factor authentication (MFA), fraud management systems (FMS), other account-
16 holder enrollment and verification processes: *Provided*, That, such risk management
17 systems and controls are proportionate and commensurate to the nature, size and
18 complexity of their operations and of the transactions involved.

19 Responsible Institutions that complied with the requirements of adequate risk
20 management systems and controls, as may be determined by the BSP, shall be
21 protected from any liability arising from any of the punishable acts defined under
22 Sections 4 and 5 of this Act: *Provided*, That, Responsible Institutions which failed to
23 comply with the requirements of adequate risk management systems and controls
24 shall be liable for any loss or damage incurred by any person arising from any of the
25 punishable acts defined under Sections 4 and 5 of this Act.

26 Consistent with existing laws, the BSP may order the payment or reimbursement of
27 money for failure of the Responsible Institutions to employ adequate risk management
28 systems and controls and exercise highest degree of diligence.

29 **SEC. 7. Temporary Holding of Disputed Transactions.-** Whenever a Responsible
30 Institution, acting upon information from another Responsible Institution, or upon a
31 complaint from an aggrieved party under this Act, or upon a finding under its own
32 FMS, suspects or has reasonable grounds to suspect that a transaction appears to be
33 unusual, has no clear economic purpose, illegal, from an illegal resource, or involves
34 proceeds from an unlawful activity or instrumentalities under this Act, regardless of
35 the amount involved, such Responsible Institution shall have the authority, within the
36 period prescribed by BSP, which shall not exceed thirty (30) calendar days, unless
37 otherwise extended by a Court of competent jurisdiction, to temporarily hold the
38 disputed funds subject of the transaction. During the said period, the Responsible
39 Institution involved, the account holder, and the other Responsible Institution/s that
40 accepted or shall accept the transfer of the disputed funds shall initiate a coordinated
41 verification process to validate the transaction. In instances where the suspicion arises

1 from the responsible institution's finding under its own FMS, the responsible institution
2 shall perform such acts as may legally be warranted to preserve the integrity of the
3 financial account and under such conditions as may be prescribed by the BSP. For this
4 purpose, the BSP shall have the authority to issue such rules and regulations on the
5 procedure for the holding of disputed funds, period of holding, and the release thereof,
6 as well as other legally permissible actions by the Responsible Institutions. Moreover,
7 for purposes of the coordinated verification by the Responsible Institutions mentioned
8 above, the provisions of Republic Act No. 1405, otherwise known as the "Secrecy of
9 Bank Deposits Law," Republic Act No. 6426, as amended, otherwise known as the
10 "Foreign Currency Deposit Act," Republic Act No. 8367, otherwise known as the
11 "Revised Non-Stock Savings and Loan Association Act of 1997," and Republic Act No.
12 10173, otherwise known as the "Data Privacy Act of 2012," shall not apply.

13 No administrative, criminal, or civil proceedings shall be imposed against any
14 Responsible Institution for holding the disputed funds mentioned above when such is
15 done in good faith, in accordance with BSP rules and regulations and whether or not
16 the transaction involving the disputed funds resulted in any criminal prosecution under
17 this Act, its IRR, or any other law.

18 Any Responsible Institution or person that held or will hold the disputed funds, or any
19 person who, with malice or in bad faith, reports or files a completely unwarranted or
20 false information that results in the holding of disputed funds shall be punishable
21 under Sections 10 and Section 11 of this Act, as the case may be.

22 **SEC. 8. Higher Penalty for Acts Committed Under the Revised Penal Code**
23 **and Crimes Under Special Laws using Money Mule and Social Engineering**
24 **Schemes.** - All crimes defined and penalized by Act No. 3815, otherwise known as
25 the Revised Penal Code, as amended, and special laws, if committed by and through
26 the acts as defined under Section 4 and Section 5 hereof, shall be covered by relevant
27 provisions of this Act: Provided, That the penalty to be imposed shall be one (1) degree
28 higher than that provided for by the Revised Penal Code, as amended, or special laws,
29 if any, or this Act, whichever is the highest.

30 **SEC. 9. Liability Under Other Laws.** - A prosecution under this Act shall be without
31 prejudice to any prosecution for violation of any provision of the Revised Penal Code,
32 as amended, or special laws, including but not limited to Republic Act Nos. 8484, 9160,
33 and 10175, as amended.

34 Prohibited Acts under Sections 4 and 5 of this Act shall be considered as "Unlawful
35 Activities" under Section 3(I) of Republic Act No. 9160, otherwise known as the "Anti-
36 Money Laundering Act of 2001," as amended.

37 **Sec. 10. Penalties.** - Any person found guilty of the punishable act under Section 4
38 (a) shall be punished with imprisonment of not less than six (6) years but not more
39 than eight (8) years, and a fine of at least One Hundred Thousand Pesos (PHP
40 100,000.00) but not exceeding Five Hundred Thousand Pesos (PHP 500,000.00).

1 Any person found guilty of any of the punishable acts enumerated in Section 4 (b)
2 shall be punished with imprisonment of not less than ten (10) years but not more than
3 twelve (12) years and a fine of at least Five Hundred Thousand Pesos (PHP
4 500,000.00) but not exceeding One Million Pesos (PHP 1,000,000.00), *Provided*, That
5 the penalty of not less than eight (8) years but not more than twelve (12) years, and
6 a fine of at least One Million Pesos (PHP 1,000,000.00) but not exceeding Two Million
7 Pesos (PHP 2,000,000.00) shall be imposed if the target or victim of the acts
8 enumerated in Section 4 (b) and is or includes a senior citizen aged sixty (60) years
9 old or above at the time the offense was committed.

10 Any person found guilty of any of the offenses that constitutes economic sabotage
11 under Section 4 (c) shall be punished with Life Imprisonment and a fine of not less
12 than One Million Pesos (PHP 1,000,000.00) but not more than Five Million Pesos (PHP
13 5,000,000.00).

14 Any person found guilty of any of the punishable acts enumerated in Section 5 shall
15 be punished with imprisonment of not less than four (4) years but not more than six
16 (6) years and a fine of at least One Hundred Thousand Pesos (PHP100,000.00) but
17 not exceeding Two Hundred Thousand Pesos (PHP200,000.00) or both, at the
18 discretion of the court.

19 Any person found guilty of committing the acts mentioned in the last paragraph of
20 Section 7 of this act shall be punished with imprisonment of not less than one (1) year
21 but not more than five (5) years or a fine of not less than Fifty Thousand Pesos (PHP
22 50,000.00) but not more than Two Hundred Thousand Pesos (PHP200,000.00), or
23 both, at the discretion of the Court. Further, the same penalty shall be imposed against
24 any person found guilty of knowingly or willfully obstructing, impeding, frustrating or
25 delaying the examination and investigation of the BSP as provided under Section 12
26 of this Act or any person found guilty of committing the acts mentioned in the
27 penultimate paragraph of Section 12 of this Act.

28 Any government official or employee who shall be found guilty of any of the unlawful
29 acts defined under Sections 4, and 5 of this act shall, in addition to the penalties
30 prescribed under this section, suffer perpetual absolute disqualification from holding
31 any appointive or elective position in the government, or in any agency, entity, or
32 instrumentality thereof.

33 **SEC. 11. Corporate Liability.** - When any of the punishable acts herein defined
34 knowingly committed on behalf of or for the benefit of a juridical person, by a natural
35 person who has a leading position within based on (a) a power of representation of
36 the juridical person: *Provided*, That the act committed falls within the scope of such
37 authority; (b) an authority to take decisions on behalf of the juridical person: *Provided*,
38 That the act committed falls within the scope of such authority; or (c) an authority to
39 exercise control within the juridical person, the juridical person shall be held liable for
40 a fine equivalent to at least double the fines imposable in Section 8 hereof up to a
41 maximum of Ten Million Pesos (PHP10,000,000.00).

1 The liability imposed on the juridical person shall be without prejudice to the criminal
2 liability of the natural person who has committed an offense under this act.

3 **Sec. 12. Enforcement** -The provisions of Chapters IV and VII of Republic Act No.
4 10175, otherwise known as the "Cybercrime Prevention Act of 2012" shall be
5 applicable in the enforcement of this Act: *Provided*, That in addition to the cybercrime
6 units of the National Bureau of Investigation (NBI) and the Philippine National Police
7 (PNP), the BSP shall have the authority to investigate cases involving violations of
8 this Act, and to apply for cybercrime warrants and orders mentioned in Chapter IV of
9 Republic Act No. 10175: *Provided*, further, That the BSP may request assistance of
10 the NBI and the PNP in the investigation of cases involving violations of this Act and
11 in the enforcement and implementation of cybercrime warrants and related orders.

12 The BSP shall have the authority to examine and investigate individual financial
13 accounts, e-wallets, or other financial accounts which are involved in the prohibited
14 acts and other offenses under Sections 4 and 5 of this Act. For this purpose, the
15 provisions of Republic Act No. 1405, otherwise known as the "Secrecy of Bank Deposits
16 Law," Republic Act No. 6426, as amended, otherwise known as the "Foreign Currency
17 Deposit Act," Republic Act No. 8367, otherwise known as the "Revised Non-Stock
18 Savings and Loan Association Act of 1997," and Republic Act No. 10173, otherwise
19 known as the "Data Privacy Act of 2012", shall not apply to other financial accounts,
20 which are subject of investigation of BSP under this provision.

21 No Court except the Court of Appeals or the Supreme Court can enjoin the BSP from
22 examining and investigating any financial account which are involved in the prohibited
23 acts and other offenses under sections 4 and 5 of this Act, unless there is convincing
24 proof that the action of the BSP is plainly arbitrary and made in bad faith.

25 No Responsible Institution, or any of its directors, officers, or employees shall be
26 subject to any action, claim, or demand in connection with, and shall be held free and
27 harmless from liability for, any act done in compliance with an order for inquiry or
28 examination of or other financial accounts from BSP: *Provided*, furthermore. That the
29 BSP may use any or all information gathered from the above inquiry, examination, or
30 investigation, in the course of its implementation of relevant provisions of Republic
31 Act No. 11765 or the "Financial Products and Services Consumer Protection Act of
32 2022".

33 It shall be unlawful, however, for any official or employee, of a Responsible Institution
34 or the BSP, to disclose any information concerning said other financial accounts to any
35 person under such conditions other than in relation to the examination and
36 investigation under this Section. It shall be unlawful for any person to use this Act for
37 persecution or harassment or as an instrument to hamper competition in trade and
38 commerce.

39 The BSP shall have the authority to issue rules on the information sharing and
40 disclosure with law enforcement and other competent authorities in connection with
41 its examination and investigation of financial, e-wallets, and other financial accounts

1 under this provision: Provided, finally, That any information which may be shared by
2 BSP under this provision shall be used solely for the investigation and prosecution of
3 cases involving the prohibited acts and other offenses defined under Section 4 and 5
4 of this Act.

5 **SEC. 13. Jurisdiction.** - The Regional Trial Court shall have jurisdiction over any
6 violation of the provisions of this Act, including any violation committed by a Filipino
7 national regardless of the place of commission. Jurisdiction shall lie if any of the
8 elements was committed within the Philippines or committed with the use of any
9 device, tool, equipment, computer system or infrastructure, wholly or partly situated
10 in the country, or when by such commission any damage is caused to a natural or
11 juridical person who, at the time the offense was committed, was in the Philippines.

12 **SEC. 14. Civil Liability in Case of Conviction.** – A conviction for violation of this
13 Act shall carry with it civil liability, which may either consist of restitution for the
14 damage done or forfeiture in favor of the aggrieved party of any unwarranted benefit
15 derived from any violation of this Act, or both, at the discretion of the courts.

16 **SEC. 15. Administrative Sanctions.** – Without prejudice to the criminal penalties
17 and civil liabilities prescribed under this Act, the administrative sanctions specified in
18 the Charter of the BSP shall be made applicable to a Responsible Institution, its
19 directors, officers, trustees, employees, or agents, for violation of this Act or any
20 related rules, regulations, orders or instructions of the BSP.

21 **SEC. 16. General Principles Relating to International Cooperation.** - All
22 relevant international instruments on international cooperation in criminal matters,
23 arrangements agreed on the basis of uniform or reciprocal legislation, and domestic
24 laws, to the widest extent possible for the purposes of investigations or proceedings
25 concerning criminal offenses related to computer systems and data, or for the
26 collection of evidence in electronic form of a criminal offense, shall be given full force
27 and effect.

28 **SEC. 17. Implementing Rules and Regulations.** - Within one (1) year from the
29 effectivity of this Act, the BSP, in coordination with the Department of Justice (DOJ),
30 Department of Information and Communications Technology (DICT), NBI, PNP,
31 Cybercrime Investigation and Coordination Center (CICC), and the Anti-Money
32 laundering Council (AMLC) shall jointly promulgate the rules and regulations to
33 effectively implement the provisions of this Act.

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

38 **SEC. 18. Separability Clause.** - If for any reason, any provision of this Act is
39 declared invalid or unconstitutional, the remaining parts or provisions not affected
40 shall remain in full force and effect.

1 **SEC. 19. Repealing Clause.** - All laws, decrees, executive orders, rules and
2 regulations or parts thereof which are contrary or inconsistent with the provisions of
3 this Act are hereby repealed, amended or modified accordingly.

4 **SEC. 20. Effectivity.** - This Act shall take effect fifteen days (15) after its publication
5 in the Official Gazette or in a national newspaper of general circulation.

6 Approved,