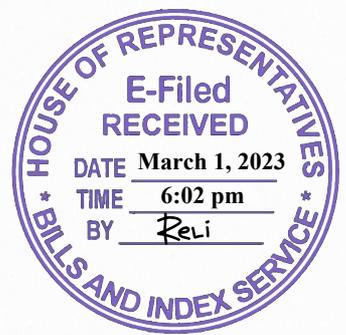


House of Representatives  
Quezon City  
NINETEENTH CONGRESS  
First Regular Session



---

**COMMITTEE REPORT No. 376**

Submitted by the Committee on Banks and Financial Intermediaries on **March 1, 2023**

Re: House Bill No. 7393

Recommending its approval in substitution of House Bills Numbered 2013 and 3172

Sponsor: Representative Tieng, Irwin, C.

---

Mr. Speaker:

The Committee on Banks and Financial Intermediaries to which were referred House Bill No. 2013, introduced by Representatives Villafuerte, Luis Raymund "Lray" Jr. F.; Villafuerte, Miguel Luis R.; Horibata, Tsuyoshi Anthony G.; Enciso, Nicholas VIII C., entitled:

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

and House Bill No. 3172, introduced by Representative Tieng, Irwin, C., entitled:

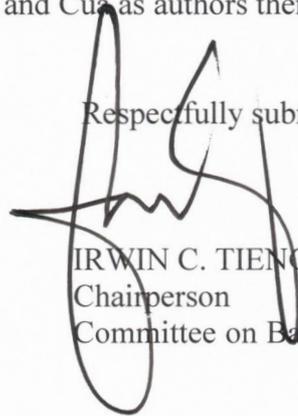
**AN ACT  
REGULATING THE USE OF BANK ACCOUNTS, ELECTRONIC WALLETS, AND  
OTHER FINANCIAL ACCOUNTS**

has considered the same and hereby recommends the approval of the attached House Bill No. 7393 entitled:

**AN ACT  
REGULATING THE USE OF FINANCIAL ACCOUNTS**

in substitution of House Bills Numbered 2013 and 3172, with Representatives Tieng, Villafuerte, LRay, Villafuerte, M., Horibata, Enciso, Rodriguez, E., Espares, Tarriela, Fariñas, Castro, F., Salceda, Bongalon, and Cuevas authors thereof.

Respectfully submitted,



IRWIN C. TIENG  
Chairperson  
Committee on Banks & Financial Intermediaries

THE SPEAKER  
HOUSE OF REPRESENTATIVES  
Quezon City



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

**NINETEENTH CONGRESS**  
**First Regular Session**

**HOUSE BILL NO. 7393**  
*(in substitution of HB2013 and HB3172)*

Introduced by Representatives Tieng, Villafuerte, LRay, Villafuerte, M., Horibata  
and Enciso

**AN ACT**  
**REGULATING THE USE OF FINANCIAL ACCOUNTS**

*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 “*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, trust,  
13 investment, credit card, and other transaction account maintained with a  
14 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 that  
20 requires the user to provide two (2) or more verification factors, such as  
21 something you know, something you have, and something you are, to gain  
22 access to a resource;
- 23 g) **Other Financial Accounts** refer to the various types of accounts used for  
24 financial transactions other than bank 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 not-  
29 for-profit;
- 30 i) **Sensitive Identifying Information** refers to any information that can be used  
31 to access an individual's financial accounts such as, usernames, passwords,  
32 bank account details, credit card, debit card, and e-wallet information among  
33 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 account or other financial account  
16 under a fictitious name or using the identity or identification  
17 documents of another to receive or transfer or withdraw  
18 proceeds derived from crimes, offenses, or social engineering  
19 schemes;  
20

21 (3) Buying or renting a financial, e-wallet or other financial  
22 account for the purpose of receiving or transferring or  
23 withdrawing proceeds derived from crimes, offenses, or social  
24 engineering schemes;  
25

26 (4) Selling and lending a financial, e-wallet or other financial  
27 account for the purpose of receiving or transferring or  
28 withdrawing proceeds derived from crimes, offenses, or social  
29 engineering schemes;  
30

31 (5) Performing account takeover or using or borrowing a financial,  
32 e-wallet, or other financial account for the purpose of receiving  
33 or transferring or withdrawing proceeds derived from crimes,  
34 offenses, or social engineering schemes; or  
35

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 the highest level of security, including  
23 multi-factor authentication (MFA), security redundancies, and other  
24 account-holder authentication and verification processes: *Provided*, That,  
25 such security levels are proportionate and commensurate to the nature, size  
26 and complexity of their operations. Subject to sufficient and undeniable  
27 proof resulting from a thorough investigation within a reasonable time,  
28 failure of these institutions to exercise proper diligence shall result to  
29 immediate 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.
- 37

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 as  
16 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 Section  
25 4(a) hereof shall be punished with imprisonment of *prision correccional* or a fine  
26 of at least One hundred thousand pesos (PhP100,000.00) but not exceeding Two  
27 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 other

1 financial accounts, which are subject of the investigation of BSP under this  
2 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

1 concerning criminal offenses related to computer systems and data, or for the  
2 collection of evidence in electronic form of a criminal offense, shall be given full  
3 force and effect.

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

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

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

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

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

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

## FACT SHEET

### House Bill No. 7393

#### **Financial Accounts Regulation Act**

*(In substitution of House Bills Numbered 2013 and 3172)*

**Introduced by:** Representatives Tieng, Villafuerte, LRay, Villafuerte, M., Horibata and Enciso

**Committee Referral:** Committee on Banks and Financial Intermediaries

**Committee Chairperson:** Representative Tieng, Irwin, C.

#### **OBJECTIVE:**

- To Protect all persons from various cybercrime schemes by regulating the use of bank accounts and e-wallets.

#### **KEY PROVISIONS**

- Prohibits and punishes financial crimes such as acting as money mule, performing social engineering schemes, and committing economic sabotage.
- Defines a money mule as a person who obtains, receives, acquires, transfers or withdraws money, funds or proceeds derived from crimes, offenses or social engineering schemes, and related prohibited acts.
- Defines social engineering scheme as the use of deception or fraudulent means by a person to obtain confidential or personal information, including sensitive identifying information of another person.
- Defines economic sabotage as a prohibited act committed by a syndicate, or committed in large scale or using a mass mailer. An act is deemed committed by a syndicate when carried out by a group of three (3) or more persons conspiring and confederating with one another. It is deemed committed in large scale when perpetrated against three (3) or more persons, individually or as a group.
- Provides that banks and other financial institutions shall ensure that access to their clients' accounts are protected by the highest level of security, including multi-factor authentication (MFA), security redundancies, and other account-holder authentication and verification processes; *Provided, that*, such security levels are proportionate and commensurate to the nature, size and complexity of their operations. Subject to sufficient and undeniable proof resulting from a thorough investigation within a reasonable time, failure of these institutions to exercise proper diligence shall result to immediate restitution of amounts lost to the rightful owners

- Provides that crimes defined and penalized under Act No. 3815, otherwise known as the Revised Penal Code, as amended, and special laws, if committed by and through the acts as defined in this Act, 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.
- Penalizes persons found guilty of acting as money mules with imprisonment of six months and one day to six years (*prision correccional*), or a fine of at least One hundred thousand pesos (Php 100,000.00) but not exceeding Two hundred thousand pesos (Php 200,000.00), or both.
- Penalizes persons performing social engineering schemes with imprisonment of six years and one day to twelve years (*prision mayor*), or a fine of at least Two hundred thousand pesos (Php 200,000.00) but not exceeding Five hundred thousand pesos (Php 500,000.00), or both. The maximum penalty shall be imposed if the victims include senior citizens aged sixty (60) years old or above.
- Penalizes persons found guilty of offenses constituting economic sabotage with life imprisonment and a fine of not less than One million pesos (Php 1,000,000.00) but not more than Five Million Pesos (Php 5,000,000.00).
- Penalizes persons found guilty of wilfully aiding and abetting or attempting to commit the prohibited acts with imprisonment one (1) degree lower than the prescribed penalty, or a fine of at least One hundred thousand pesos (Php 100,000.00) but not exceeding Five hundred thousand pesos (Php 500,000.00), or both.
- Imposes on a juridical person a fine equivalent to at least double the imposable fine up to a maximum of Ten million pesos (Php 10,000,000), where a natural person with a leading position within said juridical person knowingly commits any prohibited act on behalf of or for the benefit of the juridical person, either thru legal representation or customary authority, and said act falls within the scope of authority or control of the natural person.
- Mandates that the provisions 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.
- Empowers the *Bangko Sentral ng Pilipinas* to investigate cases involving violations of the provisions of this Act, to apply for cybercrime warrants and orders under the pertinent provisions *Republic Act No. 10175*, and to secure the assistance of law enforcement authorities in its investigation, enforcement and implementation of cybercrime warrants and related orders.

- Mandates the establishment of a cooperative mechanism among concerned government agencies, banks and covered financial institutions, private sectors and other concerned stakeholders to ensure effective prosecution of cases and enforcement of the law.
- Provides for a “*safe harbor clause*” whereby no bank or institution, or any of its directors, officers or employees, shall be subject to any action, claim or demand in connection with, and shall be held free and harmless from liability for any act done in compliance with an order for inquiry or examination of or other financial accounts from BSP.

## **RELATED LAWS**

**Act No. 3815**, as amended, also known as The Revised Penal Code

**Republic Act No. 8484**, as amended, also known as the Access Devices Regulation Act of 1998

**Republic Act No. 8791**, as amended, also known as The General Banking Law of 2000

**Republic Act No. 8792**, also known as the Electronic Commerce Act of 2000

**Republic Act No. 9160**, as amended, also known as the Anti-money Laundering Act or 2001

**Republic Act No. 10173**, also known as the Data Privacy Act of 2012

**Republic Act No. 10175**, also known as the Cybercrime Prevention Act of 2012

**Republic Act No. 11765** also known as the Financial Products and Services Consumer Protection Act of 2022