

'22 JUL 12 A10 :36

SENATE
S. No. 336

RECEIVED BY _____

Introduced by Senator Grace Poe

**AN ACT
REGULATING THE USE OF BANK ACCOUNTS, E-WALLETS, AND OTHER
FINANCIAL ACCOUNTS, PROVIDING PENALTIES THEREFOR AND FOR
OTHER PURPOSES**

EXPLANATORY NOTE

The COVID-19 pandemic has ushered the rapid growth of e-commerce and digital transactions in the country as many Filipinos—as a result of the restrictions on travel and face-to-face interaction—are forced to conduct their transactions online. The Bangko Sentral ng Pilipinas (BSP) noted that as of the third quarter of 2021, at least 41 million Filipino adults have become part of the formal financial system—with 20 million on board between 2020 and the third quarter of 2021.¹ Additionally, E-Money accounts rose by 16.8 million between 2019 to October 2021.²

Transactions coursed through Instapay—an electronic service that is designed for urgent and small value transactions—grew by 47%, or from 30.6 million transactions in 2020 to 45 million transactions by the end of 2021.³ In terms of value, Instapay also processed P289 billion-worth of transactions in 2021.⁴ The other electronic financial service, PesoNet, also reported a 26% increase in volume of transactions (from 5.5 million to 7 million transactions), and a 37% increase in terms

¹ De Vera, Ben O. (17 February 2022). "41 Million Filipinos Now Have Banking, E-Money Access". Philippine Daily Inquirer. Accessed from: <https://business.inquirer.net/341084/41m-filipinos-now-have-banking-e-money-access>

² Ibid.

³ Gonzales, Anna Leah E. (25 January 2022). "E-Payment Transactions Up in December". The Manila Times. Accessed from: <https://www.manilatimes.net/2022/01/25/business/top-business/e-payment-transactions-up-in-december/1830481>

⁴ Ibid.

of value of the transactions (from P366 billion in 2020 to P502.9 billion in 2021).⁵ Clearly, more and more Filipinos are utilizing digital avenues for financial transactions.

However, as online payment and transactions in the country continue to rise, Filipinos have increasingly become more vulnerable to crimes related to online financial transactions. BSP noted that complaints related to internet banking and mobile banking account for at least 45.2% of the total complaints received in 2021.⁶ It also reported a prominent increase in volume of concerns related to internet and mobile banking as issues related deposit, including E-Banking, became the top consumer concern in both 2020 and 2021.⁷ Similarly, TransUnion, a global information and insights company, also reported that as of March 2021, 44% of Philippine consumers have been targeted by digital fraud, while fraud attempts against businesses rose up to 31% when comparing pre-pandemic to pandemic levels.⁸

Among the cybercrimes that surged during the pandemic is *phishing*, which recently became one of the most common cyberattack mechanisms employed. BSP noted that phishing and other social engineering schemes increased by 301.83% in 2020, and that it is part of the top cybercrimes within the said year.⁹ And it continues to remain rampant to this day, with the recent news of a group of teachers becoming victims of a phishing scam, with some losing as much as P121,000 of their savings in their bank accounts.¹⁰

⁵ Ibid.

⁶ Bangko Sentral ng Pilipinas. (17 January 2021). Gov. Diokno's Opening Statement delivered during the hearing of the Senate Committee on Banks, Financial institutions & Currencies on the Financial Consumer Protection Bill.

⁷ Data from Bangko Sentral ng Pilipinas.

⁸ TransUnion. (24 March 2021). "One Year After COVID-19 Pandemic Declared, New TransUnion Research Shows Digital Fraud Attempts From the Philippines have Increased". Accessed from: <https://newsroom.transunion.ph/one-year-after-covid-19-pandemic-declared-new-transunion-research-shows-digital-fraud-attempts-from-the-philippines-have-increased/>

⁹ Bangko Sentral ng Pilipinas. (17 January 2021). Gov. Diokno's Opening Statement delivered during the hearing of the Senate Committee on Banks, Financial institutions & Currencies on the Financial Consumer Protection Bill.

¹⁰ Rivas, Ralf. (24 January 2022). "Landbank Says Teachers Fell to Phishing Scam, No Hacking". Rappler. Accessed from: <https://www.rappler.com/business/landbank-says-teachers-fell-phishing-scam-no-hacking/>

On the same note, the Anti-Money Laundering Council (AMLC) reported a rise in suspicious transaction reports (STRs) during the first 8 months of 2020, which climbed by 57%.¹¹ Nearly half (49%) of the STR filings were related to phishing and skimming, with an estimated value of Php2.7 billion, while transactions related to money mules or pass-through accounts made up 9% of the STRs, with an estimated value of Php406.9 million.¹² These money mules or pass-through accounts are often utilized to hide the proceeds derived from illegal transactions and activities.

BSP has since released a Memorandum which mandates banks and other BSP-supervised financial institutions to adopt and implement effective measures for the protection of financial consumers, including the proactive promotion of digital literacy and cybersecurity awareness as well as the institutionalization of a responsive complaint and redress mechanism for consumers.¹³ However, many of the victims express their view of the clear inadequacy of these measures.¹⁴

It is under these circumstances that the present bill must be passed. By strictly penalizing money mules and social engineering schemes, this measure seeks to ensure that the hard-earned money of the public is kept safe, and that public trust and confidence in our current financial system are maintained as it continues to innovate and traverse through cyberspace.

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



GRACE POE

¹¹ Noble, Luz Wendy T. (20 November 2020). "Suspicious Transactions Continue to Rise". Business World. Accessed from: <https://www.bworldonline.com/suspicious-transactions-continue-to-rise/>

¹² Ibid.

¹³ Bangko Sentral ng Pilipinas, Memorandum No. M-2020-053 Series of 2020, 19 June 2020.

¹⁴ Gonzales, Gelo. (28 July 2021). "Phishing Victims Turn to Class-Action Lawsuits Against Banks". *Rappler.com*. Accessed from: <https://www.rappler.com/technology/phishing-victims-class-action-lawsuits-banks>

'22 JUL 12 A10 :36

SENATE
S. No. 336



Introduced by Senator Grace Poe

AN ACT
REGULATING THE USE OF 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 “Bank Account, E-
2 wallet, and Other Financial Accounts Regulation Act”.

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

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

- 1 a. *Account Takeover* refers to a form of identity theft and fraud, where a
2 malicious third party successfully gains access and control of a user's financial
3 accounts;
- 4 b. *Bank Account* refers to an interest or non-interest bearing deposit, trust,
5 investment and other transaction account maintained with a bank or a
6 financial institution;
- 7 c. *Bulk Emailing or Mass Mailing* refers to the act of sending an electronic mail
8 (email) in mass, with at least fifty (50) or more recipients;
- 9 d. *Entity* refers to natural or juridical persons, including corporations,
10 partnerships, associations, organizations, joint ventures, government agencies
11 or instrumentalities, Government-Owned and Controlled Corporations
12 (GOCCs), or any other legal entity, whether for profit or not-for-profit;
- 13 e. *Electronic Wallet (e-wallet)* refers to a digital value stored in either a software
14 or application which the users can use for financial transactions such as
15 payments, fund transfers, top-ups or cash in and/or withdrawals, among
16 others. Example of e-wallets are e-money or virtual asset accounts stored in
17 mobile or web-based apps;
- 18 f. *Money Mule* refers to any person who obtains receives, acquires, or transfers
19 or withdraws money, funds, or proceeds derived from crimes, offenses or
20 social engineering schemes, on behalf of others, in exchange for commission
21 or fee, and those who commit the acts under Section 4(a) of this Act;
- 22 g. *Other Financial Accounts* refer to new or emerging forms of financial accounts
23 other than bank accounts and e-wallets;
- 24 h. *Phishing* refers to a social engineering scheme of posing as a legitimate or
25 trusted entity, or as a representative of a legitimate or trusted entity mainly
26 through electronic communication in order to obtain sensitive identifying
27 information of another by illegally accessing an individual's account;
- 28 i. *Sensitive Identifying Information* refers to any information that can be used
29 to access an individual's financial accounts such as, but not limited to,
30 usernames, passwords, bank account details, credit card, debit card, and e-
31 wallet information, among other electronic credentials; and

1 j. *Social Engineering Scheme*, in the context of information security, refers to
2 the use of deception or fraudulent means to obtain confidential or personal
3 information, including sensitive identifying information, of another entity. This
4 includes phishing and any of its variations such as but not limited to vishing,
5 smishing, as well as other similar forms of deception.

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

8 a. *Money mule*. It shall be prohibited for any person to act as a money mule as
9 defined under this law. The following acts shall also constitute as an offense:

- 10 1. Opening a bank account, e-wallet account or other financial account
11 and using or allowing the use thereof to receive or transfer or
12 withdraw proceeds derived from crimes, offenses or social engineering
13 schemes;
- 14 2. Opening a bank account, e-wallet account or other financial account
15 under a fictitious name or using the identity or identification documents
16 of another to receive or transfer or withdraw proceeds derived from
17 crime, offenses, or social engineering schemes;
- 18 3. Buying or renting a bank account, e-wallet account or other financial
19 account for the purpose of receiving or transferring or withdrawing
20 proceeds derived from crimes, offenses or social engineering schemes;
- 21 4. Selling a bank account, e-wallet account or other financial account for
22 the purpose of receiving or transferring or withdrawing proceeds
23 derived from crimes, offenses or social engineering schemes;
- 24 5. Account takeover or using or borrowing a bank account, e-wallet
25 account or other financial account for the purpose of receiving or
26 transferring or withdrawing proceeds derived from crimes, offenses, or
27 social engineering schemes; and
- 28 6. Recruiting, enlisting, contracting, hiring or inducing any person to act
29 as a money mule.

30 b. *Social Engineering Schemes*. Any person performing any social engineering
31 schemes as defined under Section 3 of this Act, including phishing and any
32 variations thereof, shall be penalized under this Act.

1 c. *Economic Sabotage.* Any offense defined under this Section shall be
2 considered as an offense involving economic sabotage when any of the
3 following 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 offense was committed by way of bulk email or mass mail.

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

12 Sec. 5. *Other Offenses.* – The acts involving or having relation to the
13 following shall also constitute an offense:

- 14 a. Any person who willfully abets or aids in the commission of any of the
15 offenses enumerated under Section 4 of this Act shall be held liable; and
- 16 b. Any person who willfully attempts to commit any of the offenses enumerated
17 under Section 4 of this Act shall be held liable.

18 Sec. 6. *Liability Under Other Laws.* – A prosecution under this Act shall be
19 without prejudice to any liability for violation of any provision of the Revised Penal
20 Code, as amended, or special laws.

21 Sec. 7. *Penalties.* – Any person found guilty of the punishable act under
22 Section 4(A) shall be punished with imprisonment of *prision correccional* or a fine of
23 at least One hundred thousand pesos (P100,000.00) but not exceeding Two hundred
24 thousand pesos (P200,000.00), or both.

25 Any person found guilty of any of the punishable acts enumerated in Section
26 4(B) shall be punished with imprisonment of *prision mayor* or a fine of at least Two
27 hundred thousand pesos (P200,000.00) but not exceeding Five hundred thousand
28 pesos (P500,000.00), or both: *Provided, however,* That the maximum penalty shall
29 be imposed if the target or victim of the social engineering scheme is or includes a
30 senior citizen aged sixty (60) years old or above at the time the offense was
31 committed or attempted.

1 Any person found guilty of any of the offenses that constitutes economic
2 sabotage under Section 4(C) 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
6 5 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 (P100,000.00) but not exceeding Five hundred thousand pesos (P500,000.00) or
9 both.

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

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

24 Sec. 10. *Enforcement.* – The NBI and PNP shall be responsible for the
25 efficient and effective law enforcement of the provisions of this Act. The cybercrime
26 unit or center established under Section 10 of Republic Act No. 10175 shall
27 exclusively handle all cases involving violations of this Act: *Provided,* That they shall
28 coordinate closely with the Bangko Sentral ng Pilipinas and other relevant
29 government agencies in the investigation and enforcement of cybercrime warrants
30 and related orders.

31 Sec. 11. *Response to Consumers.* – Banks, Non-Bank Financial Institutions,
32 and other pertinent Bank and Non-Bank Institutions shall immediately and effectively

1 respond to all complaints related to social engineering attacks other cybercrimes
2 perpetrated upon consumers. They shall comprehensively investigate each case,
3 provide continuous updates to consumers, coordinate with the proper authorities,
4 and exhaust all means to ensure that victims are able to recover their monetary loss,
5 if any.

6 The said institutions shall likewise institute measures to strengthen their
7 online platforms, payment systems, and data security, among others.

8 *Sec. 12. Implementing Rules and Regulations.* — Within sixty (60) days from
9 the effectivity of this Act, the Bangko Sentral ng Pilipinas (BSP), Department of
10 Justice (DOJ), Department of Information and Communications Technology (DICT),
11 National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall
12 promulgate the rules and regulations to effectively implement the provisions of this
13 Act.

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

20 Additionally, a cooperative mechanism shall be established among the
21 concerned government agencies, banks, financial and other covered institutions,
22 private and corporate sectors, and other concerned stakeholder groups to ensure
23 the effective prosecution of cases and enforcement of this Act.

24 *Sec. 13. Appropriation.* — The amount necessary for the effective
25 implementation of this Act shall be incorporated in the General Appropriations Act.

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

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

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

Approved,