



23 JAN 12 P3:31

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

RECEIVED BY:

SENATE
S.B. No. 1663

Introduced by **SENATOR IMEE R. MARCOS**

AN ACT
PENALIZING FINTECH CRIME, PROVIDING PENALTIES
THEREFOR, AND FOR OTHER PURPOSES

EXPLANATORY NOTE

The Philippines is host to approximately 79 million mobile phone users as of August 2022.¹ Of this statistic, about 20 million Filipinos use electronic wallets (e-wallets), which is a significant fraction of the country's total population of just over 100 million.² The pandemic likewise resulted in a 52% increase in the number of Filipinos who shop online.³

As ever-renewing financial technologies ("fintech") permeate Philippine society, new ways of perpetrating financial crime, enabled by these technologies, also emerge. The introduction of fintech has spiked the commission of cybercrimes that take advantage of technologies to perpetrate phishing and launder money. Top examples that pervade today's news are e-commerce scams, loan scams, credit-for-sex scams, and internet love scams. While banks and other financial institutions have been mandated by the *Bangko Sentral ng Pilipinas* (BSP) via various memoranda to adopt measures to protect financial consumers, the enactment of a supporting law is needed to fully mitigate fintech-related crimes.

This bill seeks to define and penalize fintech-related offenses to raise awareness of their occurrence and significantly deter their commission. Moreover, in view of their damaging effects on the economy, the bill seeks to declare the commission of certain fintech crimes, when done in large scale, as a form of economic sabotage and a heinous

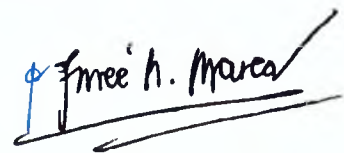
¹ "E-Wallets and Anti-Money Laundering in the Philippines" 17 August 2022. Tookitaki Thanos Co. <https://www.tookitaki.com/blog/news-views/e-wallets-and-anti-money-laundering-in-the-philippines>

² "GCash is building a cashless ecosystem" GCash website. <https://www.gcash.com/#:~:text=As%20of%202019%2C%20GCash%20has,partner%20merchants%20across%20the%20country>

³ *Id.* at 1.

crime punishable by the maximum penalty allowed by law. The emerging new market of fintech should be taken full advantage of for its gains and not utilized for the enhanced perpetration of online crime.

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

A handwritten signature in blue ink that reads "Imee R. Marcos". The signature is written in a cursive style and is positioned above a horizontal line.

IMEE R. MARCOS



23 JAN 12 P3:32

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

RECEIVED BY:

SENATE
S.B. No. 1663

Introduced by **SENATOR IMEE R. MARCOS**

**AN ACT
PENALIZING FINTECH CRIME, 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 ‘*Fintech Crime Prevention*
2 *Act of 2023*’.

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

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

20 a. *Account Takeover* refers to a form of identity theft and fraud, where a
21 malicious third party successfully gains access and control of a user's financial accounts;

22 b. *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;

25 c. *Bulk Emailing* or *Mass Mailing* refers to the act of sending an electronic mail
26 (e-mail) in mass, with at least fifty (50) or more recipients;

1 d. *Entity* refers to natural or juridical persons, including corporations,
2 partnerships, associations, organizations, joint ventures, government agencies or
3 instrumentalities, Government-Owned and -Controlled Corporations (GOCCs), or any
4 other legal entity, whether for profit or not-for-profit;

5 e. *Electronic Money (E-Money)* shall refer to a monetary value stored in a
6 transaction account that is not a deposit and non-interest-bearing that was issued,
7 created, or accepted by a bank - and is:

8 i. electronically-stored in an instrument or device;

9 ii. denominated in or pegged to the Philippine Peso or other foreign
10 currencies;

11 iii. pre-funded by customers to enable payment transactions through the use
12 of a transaction account;

13 iv. accepted as a means of payment by the issuer for its customers or by
14 other persons or entities including merchants/sellers;

15 v. issues against receipt of funds of an amount equal to the monetary value
16 issued; and

17 vi. withdrawable in cash or cash equivalent or transferrable to other
18 accounts/instruments that are withdrawable in cash.

19 f. *Electronic Wallet (E-wallet)* refers to a digital value stored in either a software
20 or application which the users can use for financial transactions such as payments, fund
21 transfers, top-ups or cash in and/or withdrawals, among others. Example of e-wallets
22 are e-money or virtual asset accounts stored in mobile or web-based apps;

23 g. *Financial Technology (Fintech)* refers to new technology that improves and
24 automates the delivery and use of financial services;

25 h. *Money Mule* refers to any person who obtains receives, acquires, or transfers
26 or withdraws money, funds, or proceeds derived from crimes, offenses or social
27 engineering schemes, on behalf of others, in exchange for commission or fee, and
28 those who commit the acts under Section 4(a) of this Act;

29 i. *Other Financial Accounts* refer to new or emerging forms of financial accounts
30 other than bank accounts and e-wallets;

31 j. *Phishing* refers to a social engineering scheme of posing as a legitimate or
32 trusted entity, or as a representative of a legitimate or trusted entity mainly through
33 electronic communication In order to obtain sensitive identifying information of another
34 by illegally accessing an individual's account;

35 k. *Sensitive Identifying Information* refers to any information that can be used
36 to access an Individual's financial accounts such as, but not limited to usernames,
37 passwords, bank account details, credit card, debit card, and e31 wallet information,
38 among other electronic credentials; and

39 l. *Social Engineering Scheme*, in the context of information security, refers to
40 the use of deception or fraudulent means to obtain confidential or personal information,
41 including sensitive identifying information, of another entity. This includes phishing and

1 any of its variations such as but not limited to vishing, smishing, as well as other similar
2 forms of deception.

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

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

8 1. Opening a bank account, e-wallet account or other financial account and using
9 or allowing the use thereof to receive or transfer or withdraw proceeds derived
10 from crimes, offenses or social engineering schemes;

11 2. Opening a bank account, e-wallet account or other financial account under a
12 fictitious name or using the identity or identification documents of another to
13 receive or transfer or withdraw proceeds derived from crime, offenses, or social
14 engineering schemes;

15 3. Buying or renting a bank account, e-wallet account or other financial account
16 for the purpose of receiving or transferring or withdrawing proceeds derived
17 from crimes, offenses or social engineering schemes;

18 4. Selling a bank account, e-wallet account or other financial account for the
19 purpose of receiving or transferring or withdrawing proceeds derived from
20 crimes, offenses or social engineering schemes;

21 5. Account takeover or using or borrowing a bank account, e-wallet account or
22 other financial account for the purpose of receiving or transferring or
23 withdrawing proceeds derived from crimes, offenses, or social engineering
24 schemes; and

25 6. Recruiting, enlisting, contracting, hiring or inducing any person to act as a
26 money mule.

27
28 b. *Social Engineering Schemes.* Any person performing any social engineering
29 schemes, including phishing and any variations thereof, shall be penalized under this
30 Act.

31 Social engineering scheme shall be deemed committed when a person performs
32 any of the following:

33
34 (1) Makes any communication to another person by representing one's self as a
35 representative of a financial institution in order to gain the trust of others; and

36
37 (2) Uses electronic communication to induce or request any person to provide
38 sensitive identifying information with the intent to defraud or injure any person.

39
40 Banks and other financial institutions shall ensure that access to their clients'
41 accounts are protected by the highest level of security, including biometric
42 authentication, security redundancies, and other account-holder authentication and
43 verification processes. Failure of these institutions to exercise proper diligence shall
44 result to immediate restitution of amounts lost.

1 c. *Economic Sabotage.* Any offense defined under this Section shall be
2 considered 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 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 offense
8 was carried out by a group of three (3) or more persons conspiring or confederating
9 with one another, while an act shall be deemed committed in large scale if the offense
10 was committed against three (3) or more persons individually or as a group.

11
12 **Sec. 5. *Other Offenses.*** – The acts involving or having relation to the following
13 shall also constitute an offense:

14 a. Any person who willfully abets or aids in the commission of any of the offenses
15 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
19 **SEC. 6. *Higher Penalty for Acts Committed Under the Revised Penal Code and***
20 ***Crimes Under Special Laws Using Money Mule and Social Engineering Schemes.*** – All
21 crimes defined and penalized by Republic Act No. 3815, otherwise known as the
22 “Revised Penal Code”, as amended, and special laws, if committed by and through the
23 acts as defined under Section 4 hereof, shall be covered by the relevant provisions of
24 this Act: *Provided*, That the penalty to be imposed shall be one (1) degree higher than
25 that provided by the Revised Penal Code, as amended, and special laws, as the case
26 may be.

27
28 **Sec. 7. *Liability Under Other Laws.*** – A prosecution under this Act shall be
29 without prejudice to any liability for violation of any provision of the Revised Penal
30 Code, as amended, or special laws.

31
32 **Sec. 8. *Penalties.*** – Any person found guilty of the punishable act under Section
33 4(A) shall be punished with imprisonment of *prision correccional* or a fine of at least
34 One hundred thousand pesos (Php 100,000.00) but not exceeding Two hundred
35 thousand pesos (Php 200,000.00), or both.

36 Any person found guilty of any of the punishable acts enumerated in Section
37 4(B) shall be punished with imprisonment of *prision mayor* or a fine of at least Two
38 hundred thousand pesos (Php 200,000.00) but not exceeding Five hundred thousand
39 pesos (Php 500,000.00), or both: *Provided*, however, That the maximum penalty shall
40 be imposed if the target or victim of the social engineering scheme is or includes a
41 senior citizen aged sixty (60) years old or above, a minor, insane, or imbecile at the
42 time the offense was committed or attempted.

43 Any person found guilty of any of the offenses that constitutes economic
44 sabotage under Section 4(C) shall be punished with life imprisonment and a fine of not

1 less than One million pesos (Php 1,000,000.00) but not more than Five Million Pesos
2 (Php 5,000,000.00).

3 Any person found guilty of any of the punishable acts enumerated in Section 5
4 shall be punished with imprisonment one (1) degree lower than that of the prescribed
5 penalty for the offense or a fine of at least One hundred thousand pesos (Php
6 100,000.00) but not exceeding Five hundred thousand pesos (Php 500,000.00) or both.

7
8 **Sec. 9. Jurisdiction.** – The Regional Trial Court (RTC), designated as cybercrime
9 court, shall have jurisdiction over any violation of the provisions of this Act, including
10 any violation committed by a Filipino national regardless of the place of commission.
11 Jurisdiction shall lie If any of the elements was committed within the Philippines or
12 committed with the use of any computer system wholly or partly situated in the country,
13 or when by such commission any damage is caused to a natural or juridical person
14 who, at the time the offense was committed, was in the Philippines.

15
16 **Sec. 10. Freezing of Financial Account.** – Upon verified complaint by an
17 aggrieved party under this Act and after determination that probable cause exists that
18 any unlawful activity as defined in Section 4 hereof has been committed, the RTC may
19 issue a freeze order of any financial account identified to have been used in the
20 commission of the crime, which shall be effective immediately. The freeze order shall
21 be for a period of twenty (20) days unless extended by the court. In any case, the
22 court should act on any petition to freeze within twenty-four (24) hours from the filing
23 thereof. A person or entity whose account has been frozen may file a motion to lift the
24 freeze order which the court must resolve before the expiration of the twenty (20)-day
25 original freeze order.

26
27 **Sec. 11. General Principles Relating to International Cooperation.** – All relevant
28 international instruments on international cooperation in criminal matters,
29 arrangements agreed on the basis of uniform or reciprocal legislation, and domestic
30 laws, to the widest extent possible for the purposes of investigations or proceedings
31 concerning criminal offenses related to computer systems and data, or for the collection
32 of evidence in electronic form of a criminal offense, shall be given full force and effect.

33
34 **Sec. 12. Enforcement.** – The NBI and PNP shall be responsible for the efficient
35 and effective law enforcement of the provisions of this Act. The cybercrime unit or
36 center established under Section 10 of Republic Act No. 10175 shall exclusively handle
37 all cases involving violations of this Act: *Provided*, That they shall coordinate closely
38 with the *Bangko Sentral ng Pilipinas* and other relevant government agencies in the
39 investigation and enforcement of cybercrime warrants and related orders.

40
41 **Sec. 13. Response to Consumers.** – Banks, Non-Bank Financial Institutions, and
42 other pertinent Bank and Non-Bank Institutions shall immediately and effectively
43 respond to all complaints related to social engineering attacks other cybercrimes
44 perpetrated upon consumers. They shall comprehensively investigate each case,

1 provide continuous updates to consumers, coordinate with the proper authorities, and
2 exhaust all means to ensure that victims are able to recover their monetary loss, if any.

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

5
6 **Sec. 14. *Implementing Rules and Regulations.*** — Within sixty (60) days from
7 the effectivity of this Act, the *Bangko Sentral ng Pilipinas*, Anti-Money Laundering
8 Council (AMLC), Department of Justice (DOJ), Department of Information and
9 Communications Technology (DICT), National Bureau of Investigation (NBI) and the
10 Philippine National Police (PNP) shall promulgate the rules and regulations to effectively
11 implement the provisions of this Act.

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

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

22
23 **Sec. 15. *Appropriation.*** — The amount necessary for the effective
24 implementation of this Act shall be incorporated in the General Appropriations Act.

25
26 **Sec. 16. *Separability Clause.*** — If for any reason, any provision of this Act is
27 declared invalid or unconstitutional, the remaining parts or provisions not affected shall
28 remain in full force and effect.

29
30 **Sec. 17. *Repealing Clause.*** — All laws, decrees, executive orders, rules and
31 regulations or parts thereof which are contrary or inconsistent with the provisions of
32 this Act are hereby repealed, amended or modified accordingly.

33
34 **Sec. 18. *Effectivity.*** — This Act shall take effect fifteen (15) days after its
35 publication in the Official Gazette or in a newspaper of general circulation.

36
Approved,