NINETEENTH CONGRESS OF THE REPUBLIC OF THE PHILIPPINES
Second Regular Session

SENATE

S.B. No. 2407

Introduced by SEN. WIN GATCHALIAN

AN ACT
PROHIBITING MONEY MULES AND OTHER FRAUDULENT ACTS COMMITTED INVOLVING FINANCIAL ACCOUNTS, PROVIDING PENALTIES AND FOR OTHER PURPOSES

EXPLANATORY NOTE

The COVID-19 pandemic has highlighted the significance of cashless transactions and digital payments. With the convenience and ease of being able to shop, pay bills, and conduct financial transactions anywhere, more and more Filipinos are expected to rely more and more on digital financial services, such as online banking, digital banking and electronic wallets. In fact, the *Bangko Sentral ng Pilipinas'* (BSP) 2021 Demand Side data[1] shows an 80% increase in the number of internet/mobile phone users who use digital financial services from 12% in 2019 to 60% in 2021. Meanwhile, BSP's 2021 Financial Inclusion Survey also indicates that e-money accounts rose to 36% in 2021 from 8% in 2019.

With the rapid growth and popularity of digital financial services, the rise of financial-related cybercrimes followed. Cybercriminals started taking advantage of technologies to transfer illicit or stolen funds across digital financial services, stealing vital information about accountholders and taking over their accounts, or enticing accountholders with gifts or incentives with the goal of covertly committing financial crimes.

For the past three years, the unsuspecting public lost millions of their hard-earned money from these cybercriminals. A number of notable cases include the "Mark Nagoyo" scam, in which more than 700 BDO Unibank customers' accounts were

---

[1] 2022 Annual Report National Strategy for Financial Inclusion; Available at https://www.bsp.gov.ph/Pages/InclusiveFinance/2022NSFIAnnualReport.pdf; Last accessed on July 28, 2023.

hacked in late 2021[2], the unauthorized bank transfers that targeted government teachers with Landbank accounts in January 2022 wherein the victims lost between Php 26,000 to Php 121,000 from the incident[3], and the massive phishing incident involving Gcash users in May 2023[4].

As members of the financial services industry strengthen their defenses against cyberthreats, threat actors continuously come up with ingenious ways to commit financial-related cybercrimes, making use of money mules and social engineering schemes to create layers of distance between victims and criminals, thereby, making it harder for law enforcement to accurately trace money trails. Also, operations of cybercriminals grew in large scale, especially this pandemic, taking advantage of the unemployed, those who are looking for easy money, those who are unaware, and those who are willing to help others, and thriving in jurisdictions with very weak enforcement and penalties, like the Philippines. In fact, Kaspersky Security Network's 2022 Report shows that the Philippines ranked 2nd globally among countries most attacked by web threats from January to December 2022 and that the most preferred attack method by threat actors includes social engineering schemes[5].

Accordingly, it is high time to legislate a measure that penalizes those who willingly allow themselves to be used as money mules, those who use social engineering schemes and other fraudulent schemes involving financial accounts, including account takeover, recruiting or enlisting others to commit these acts, and those who commit these acts in large scale or equivalent to economic sabotage that threatens the safety of the financial accounts of Filipinos and the integrity of the country's financial system. As we continue to promote digitalization and financial inclusion, it is crucial that we prevent further social and economic consequences arising from financial-related cybercrimes.

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

WIN GATCHALIAN

---

[2] RAPPLER. "BDO Clients Lose Money Due to Alleged Online Banking Hack," December 12, 2021. Available at https://www.rappler.com/business/bdo-clients-lose-money-due-alleged-online-banking-hack/; Last accessed on July 28, 2023.

[3] Vera, Ben O. de. "Landbank: Teachers Who Lost Money Fell Victims to Phishing Scam." INQUIRER.net, January 24, 2022. Available at https://business.inquirer.net/339463/landbank-teachers-who-lost-money-fell-victims-to-phishing-scam; Last accessed on July 28, 2023.

[4] Olandres, Abe. Yugatech: "Gcash: Full explanation of Massive Phishing Incident," May 14, 2023. Available at https://www.yugatech.com/fintech/gcash-full-explanation-of-massive-phishing-incident/; Last accessed on July 28, 2023.

[5] Ronda, Rainier Allan. "'Philippines 2nd Most Attacked by Web Threats Worldwide Last Year.'" Philstar.com. March 15, 2023. Available at https://www.philstar.com/headlines/2023/03/15/2251710/philippines-2nd-most-attacked-web-threats-worldwide-last-year. Last accessed on July 28, 2023

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

SENATE

S. B. No. 2407

Introduced by SEN. WIN GATCHALIAN

AN ACT
PROHIBITING MONEY MULES AND OTHER FRAUDULENT ACTS COMMITTED INVOLVING FINANCIAL ACCOUNTS, PROVIDING PENALTIES AND FOR OTHER PURPOSES

Be it enacted by the Senate and the House of Representatives of the Philippines in Congress assembled:

SECTION 1. ***Short Title*** - This Act shall be known as the "*Anti-Financial Account Scamming Act*".

SEC. 2. ***Declaration of Policy.*** – It is hereby declared the policy of the State to protect and preserve the integrity of the country's financial system and to ensure that financial accounts and their owners are protected from and are not exploited or lured by cybercriminals or criminal syndicates into the commission of an unlawful or fraudulent activity.

Recognizing the shared role of financial service providers, and the general public in promoting and maintaining a stable and efficient financial system, the increased use of digital or electronic mediums in financial transactions, and the evolving advances in technology, the State shall enhance further the efficacy of the law against unlawful activities that use financial accounts or e-wallets to conceal or disguise the nature, location, source, ownership or control of a fraudulent or illegal activity, or that provide means or conduits to facilitate the unauthorized, illegal or fraudulent access thereof.

The State shall likewise ensure that proper mechanisms and measures are in place, including an intensive and unrelenting campaign against money mules and other fraudulent schemes, to protect the public from such unlawful activities that undermine the integrity of the country's financial system.

Due to its deleterious effect on the economy, it is the policy of the State to severely punish the large-scale commission of certain crimes in this Act with the maximum level of penalty allowed by law.

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

(a) Account owner refers to the owner or owners of a financial account as opened or registered with the financial service provider;

(b) Account takeover refers to the use of any means, such as but not limited to force, intimidation, manipulation, or deceit, whereby a malicious third party successfully gains access and control over an account owner's financial account;

(c) Bulk email refers to the volume of electronic mail sent in mass or to fifty (50) or more emails;

(d) Electronic Wallet or E-wallet refers to a digital value stored in a wallet as may be defined by the Bangko Sentral ng Pilipinas (BSP) regulations;

(e) Financial Account refers to any account that represents financial products or services developed or marketed by a financial service provider, which may include, but are not limited to, savings, interest or non-interest-bearing deposit, trust, investment, credit card, and other transaction account maintained with a bank, non-bank, or financial institution, electronic wallets and various types of accounts used for financial transactions. This also includes an account that represents digital financial products or services which pertain to the broad range of financial services accessed and delivered through online or digital channels or platforms;

(f) Financial regulator refers to the Bangko Sentral ng Pilipinas, Securities and Exchange Commission, Insurance Commission, and the Cooperative Development Authority;

(g) Financial Service Provider refers to a person which provides financial products or services as defined in Republic Act No. 11765, otherwise known as the "*Financial Products and Services Consumer Protection Act.*"

(h) Mass mailer refers to a service or software used to send electronic mail in mass or to fifty or more emails;

(i) Money mule refers to any person who obtains, receives, acquires, or transfers or withdraws money, funds, or proceeds derived from crimes, offenses, or social engineering schemes, and those who commit the prohibited acts under Section 4(a) of this Act;

(j) Multi-Factor Authentication (MFA) refers to an authentication method that requires the user to provide two (2) or more verification factors, such as something you know, something you have, and something you are, to gain access to a resource;

(k) Persons refer to natural or juridical persons, including corporations, partnerships, associations, organizations, joint ventures, government agencies or instrumentalities, government-owned and controlled corporations (GOCCs), or any other legal entity, whether for profit or not-for-profit;

(l) Sensitive Identifying Information refers to any information that can be used to access a financial account such as but not limited to, usernames, passwords, bank account details, credit card, debit card, and e-wallet information among other electronic credentials; and

(m) Social engineering scheme refers to the use of deception, misrepresentation or other fraudulent means by a person to obtain confidential or personal information, including sensitive identifying information, of another person or to manipulate another person to perform an act involving that or other person's financial account which would not otherwise be done had the true circumstances been known

and not obscured, and those acts enumerated under Section 4(b) of this Act.

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

(a) ***Money mule.*** - It shall be prohibited for any person to act as a money mule. Any person performing any of the following acts shall be considered as a money mule:

(1) Registers or opens a financial account and uses or allows the use thereof, to receive or transfer or withdraw proceeds known to be derived from crimes, offenses, or social engineering schemes;

(2) Registers or opens a financial account under a fictitious name or using the identity or identification documents of another to receive or transfer or withdraw proceeds derived from crimes, offenses, or social engineering schemes;

(3) Buys or leases a financial account for the purpose of receiving or transferring or withdrawing proceeds derived from crimes, offenses, or social engineering schemes;

(4) Sells or lends a financial account for the purpose of receiving or transferring or withdrawing proceeds derived from crimes, offenses, or social engineering schemes;

(5) Uses a financial account fraudulently applied for;

(6) Obtains money or anything of value through the use of a financial account with intent to defraud or with intent to gain and fleeing thereafter;

(7) Effects a transaction, using a financial account belonging to another person, to receive payment or any other thing of value derived from crimes, offenses, or social engineering schemes; or

(b) ***Social engineering schemes.*** - Any person performing any social engineering scheme shall be penalized under this Act. Social engineering scheme shall also be deemed committed when a person performs any of the following:

(1) Makes any communication to another person by falsely representing one's self as a representative or agent of a financial service provider or making any false representation in order to gain the trust of others and soliciting sensitive identifying information that results in account takeover;

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

(3) Causes any person to provide sensitive identifying information with the intent to defraud or with the intent to gain and fleeing thereafter.

Banks and other financial institutions shall ensure that access to their clients' accounts are protected by appropriate level of security, including, but not limited to, multi-factor authentication (MFA), 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.

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

(1) The offense was committed by a syndicate;

(2) The offense was committed in large scale;

(3) The offense was committed using a mass mailer or other similar tools used to send bulk emails or SMS, generative artificial intelligence or any similar technology that takes advantage of the reach, open access and processing power available through the internet to (a) collect and process large amounts of data, (b) break secure passwrods and encrypted data, (c) replicate likeness and voices of natural persons, (d) create fake identities, likenesses, and voices,

and (e) other analogous uses that apply new technology to cause widespread damage to the public;

(4) The offense was committed by a group of foreign nationals operating inside and outside the Philippines;

(5) The offense was committed through human trafficking.

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

SEC. 5. ***Other Offenses***. – The acts involving or having relation to the following shall also constitute an offense punishable under this Act:

(a) Performs account takeover or uses or borrows a financial account for the purpose of receiving or transferring or withdrawing proceeds derived from crimes, offenses, or social engineering schemes;

(b) Recruiting, enlisting, contracting, hiring, utilizing or inducing any person to perform the acts mentioned in Section 4(a) of this Act;

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

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

SEC. 6. ***Higher Penalty for Acts Committed Under the Revised Penal Code and Crimes Under Special Laws Using Money Mule and Social Engineering Schemes***. – All crimes defined and penalized by Act No. 3815, otherwise known as the Revised Penal Code, as amended, and special laws, if committed by and through the acts as defined under Section 4 hereof, 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.

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

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

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

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

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

SEC. 9. *Corporate Liability.* – When any of the punishable acts herein defined knowingly committed on behalf of or for the benefit of a juridical person, by a natural person who has a leading position within based on (a) a power of representation of the juridical person: *Provided*, That the act committed falls within the scope of such authority; (b) an authority to take decisions on behalf of the juridical person: *Provided*, That the act committed falls within the scope of such authority; or (c) an authority to exercise control

within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 8 hereof up to a maximum of Ten million pesos (PhP10,000,000).

SEC. 10. ***Enforcement.*** – The provision 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*: Provided*, That, in addition to the cybercrime units of the National Bureau of Investigation (NBI) and the Philippine National Police (PNP), the financial regulator shall have the authority to investigate cases involving violations of this Act, and to apply for cybercrime warrants and orders mentioned in Chapter IV of Republic Act No. 10175: *Provided, further,* That the financial regulator may request assistance of the NBI and PNP in the investigation of cases involving violations of this Act and in the enforcement and implementation of cybercrime warrants and related orders.

The financial regulator shall have the authority to examine and investigate individual financial accounts which are involved in the prohibited acts and other offenses under Sections 4 and 5 of this Act. For this purpose, the provisions of Republic Act No. 1405, otherwise known as the "Secrecy of Bank Deposits Law," Republic Act No. 6426, as amended, otherwise known as the "Foreign Currency Deposit Act," and Republic Act No. 10173, otherwise known as the "Data Privacy Act of 2012," shall not apply to financial accounts, which are subject of the investigation of financial regulator under this provision.

No financial service provider, 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 financial accounts from financial regulators: *Provided, further*, That, the financial regulator may use any or all information gathered from the above inquiry, examination or investigation, in the course of its implementation of relevant provisions of Republic Act No. 11765 or the "Financial Products and Services Consumer Protection Act of 2022."

It shall be unlawful, however, for any official or employee, of a financial service provider or the financial regulator, to disclose any information concerning said other financial accounts to any person under such conditions other than in relation to the examination and investigation under this Section. It shall be unlawful for any person to use this Act for persecution or harassment or as an instrument to hamper competition in trade and commerce.

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

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

SEC. 12. ***General Principles Relating to International Cooperation.*** – All relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense, shall be given full force and effect.

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

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

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

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

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

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

Approved,

NINETEENTH CONGRESS OF THE]
REPUBLIC OF THE PHILIPPINES]
Second Regular Session **]**

SENATE

S.B. No. _____

Introduced by SEN. WIN GATCHALIAN

AN ACT
PROHIBITING MONEY MULES AND OTHER FRAUDULENT ACTS COMMITTED INVOLVING FINANCIAL ACCOUNTS, PROVIDING PENALTIES AND FOR OTHER PURPOSES

EXPLANATORY NOTE

The COVID-19 pandemic has highlighted the significance of cashless transactions and digital payments. With the convenience and ease of being able to shop, pay bills, and conduct financial transactions anywhere, more and more Filipinos are expected to rely more and more on digital financial services, such as online banking, digital banking and electronic wallets. In fact, the *Bangko Sentral ng Pilipinas'* (BSP) 2021 Demand Side data[1] shows an 80% increase in the number of internet/mobile phone users who use digital financial services from 12% in 2019 to 60% in 2021. Meanwhile, BSP's 2021 Financial Inclusion Survey also indicates that e-money accounts rose to 36% in 2021 from 8% in 2019.

With the rapid growth and popularity of digital financial services, the rise of financial-related cybercrimes followed. Cybercriminals started taking advantage of technologies to transfer illicit or stolen funds across digital financial services, stealing vital information about accountholders and taking over their accounts, or enticing accountholders with gifts or incentives with the goal of covertly committing financial crimes.

For the past three years, the unsuspecting public lost millions of their hard-earned money from these cybercriminals. A number of notable cases include the "Mark Nagoyo" scam, in which more than 700 BDO Unibank customers' accounts were

---

[1] 2022 Annual Report National Strategy for Financial Inclusion; Available at https://www.bsp.gov.ph/Pages/InclusiveFinance/2022NSFIAnnualReport.pdf; Last accessed on July 28, 2023.

hacked in late 2021[2], the unauthorized bank transfers that targeted government teachers with Landbank accounts in January 2022 wherein the victims lost between Php 26,000 to Php 121,000 from the incident[3], and the massive phishing incident involving Gcash users in May 2023[4].

As members of the financial services industry strengthen their defenses against cyberthreats, threat actors continuously come up with ingenious ways to commit financial-related cybercrimes, making use of money mules and social engineering schemes to create layers of distance between victims and criminals, thereby, making it harder for law enforcement to accurately trace money trails. Also, operations of cybercriminals grew in large scale, especially this pandemic, taking advantage of the unemployed, those who are looking for easy money, those who are unaware, and those who are willing to help others, and thriving in jurisdictions with very weak enforcement and penalties, like the Philippines. In fact, Kaspersky Security Network's 2022 Report shows that the Philippines ranked 2nd globally among countries most attacked by web threats from January to December 2022 and that the most preferred attack method by threat actors includes social engineering schemes[5].

Accordingly, it is high time to legislate a measure that penalizes those who willingly allow themselves to be used as money mules, those who use social engineering schemes and other fraudulent schemes involving financial accounts, including account takeover, recruiting or enlisting others to commit these acts, and those who commit these acts in large scale or equivalent to economic sabotage that threatens the safety of the financial accounts of Filipinos and the integrity of the country's financial system. As we continue to promote digitalization and financial inclusion, it is crucial that we prevent further social and economic consequences arising from financial-related cybercrimes.

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

WIN GATCHALIAN

---

[2] RAPPLER. "BDO Clients Lose Money Due to Alleged Online Banking Hack," December 12, 2021. Available at https://www.rappler.com/business/bdo-clients-lose-money-due-alleged-online-banking-hack/; Last accessed on July 28, 2023.

[3] Vera, Ben O. de. "Landbank: Teachers Who Lost Money Fell Victims to Phishing Scam." INQUIRER.net, January 24, 2022. Available at https://business.inquirer.net/339463/landbank-teachers-who-lost-money-fell-victims-to-phishing-scam; Last accessed on July 28, 2023.

[4] Olandres, Abe. Yugatech: "Gcash: Full explanation of Massive Phishing Incident," May 14, 2023. Available at https://www.yugatech.com/fintech/gcash-full-explanation-of-massive-phishing-incident/; Last accessed on July 28, 2023.

[5] Ronda, Rainier Allan. "'Philippines 2nd Most Attacked by Web Threats Worldwide Last Year.'" Philstar.com. March 15, 2023. Available at https://www.philstar.com/headlines/2023/03/15/2251710/philippines-2nd-most-attacked-web-threats-worldwide-last-year. Last accessed on July 28, 2023