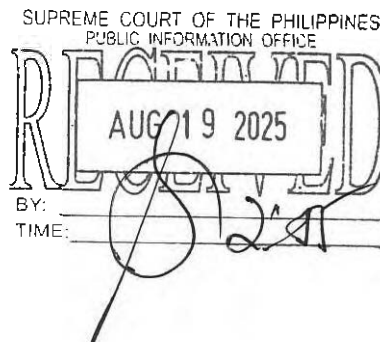




Republic of the Philippines
Supreme Court
Manila



FIRST DIVISION

EASTWEST RURAL BANK,
Petitioner,

G.R. No. 273720

Present:

- versus -

GESMUNDO, C.J.,
Chairperson,
HERNANDO,
ZALAMEDA,
ROSARIO, and
MARQUEZ, JJ.

PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
REGIONAL ANTI-CYBERCRIME
UNIT 1, represented by PAT.
RODALYN V. BAAWA,
Respondents.

Promulgated:

JUL 29 2025

X -----X

DECISION

HERNANDO, J.:

This is a Petition for Review on *Certiorari*¹ filed under Rule 45 of the Rules of Court, seeking to reverse and set aside the Resolutions dated September 26, 2023,² and April 30, 2024,³ of the Court of Appeals (CA) in CA G.R. SP. No. 180524, and to annul the Regional Trial Court (RTC) Orders dated July 3, 2023,⁴ and July 27, 2023,⁵ in WDCD No. 15-2023, for having been

¹ *Rollo*, pp. 20–46.

² *Id.* at 8–11. The September 26, 2023 Resolution in CA G.R. SP No. 180524 was penned by Associate Justice Maria Elisa Sempio Diy and concurred in by Associate Justices Angelene Mary W. Quimpo-Sale and Roberto P. Quiroz of the Special Fifteenth Division, Court of Appeals, Manila.

³ *Id.* at 13–16. The April 30, 2024 Resolution in CA G.R. SP No. 180524 was penned by Associate Justice Maria Elisa Sempio Diy and concurred in by Associate Justices Angelene Mary W. Quimpo-Sale and Roberto P. Quiroz of the Former Special Fifteenth Division, Court of Appeals, Manila.

⁴ *Id.* at 107–108. The July 3, 2023 Order in WDCD No. 15-2023 was penned by Executive Judge Victor O. Concepcion of the Office of the Executive Judge, Regional Trial Court, San Fernando City, La Union.

⁵ *Id.* at 118–119. The July 27, 2023 Order in WDCD No. 15-2023 was penned by Presiding Judge Victor O. Concepcion of Branch 66, Regional Trial Court, San Fernando City, La Union.

issued with grave abuse of discretion amounting to a lack or excess of jurisdiction.

The Factual Antecedents

The case stemmed from a complaint lodged by Leonard Vendiola y Baguio (Vendiola) with respondent Philippine National Police Anti-Cybercrime Group, Regional Anti-Cybercrime Unit 1 (PNP-ACG RACU 1) located at Camp Diego Silang, Carlatan, San Fernando City, La Union. Vendiola asserted that on May 19, 2023, at approximately 2:19 p.m., he received a phone call from a certain Justine Dela Cruz (Dela Cruz), who purported to be an employee of Banco de Oro (BDO). During the call, Dela Cruz informed Vendiola about “points” he could redeem, including an umbrella, tumbler, and planner, contingent upon Vendiola providing his email address and one-time password (OTP). Eager to obtain the promised rewards, Vendiola acquiesced and shared his email address and OTP with Dela Cruz. Upon later reviewing his BDO account via online banking, Vendiola discovered a transfer of PHP 10,000.00 to an East West Rural Bank (EWRB) account number 500023412872. He promptly reported this incident to BDO.⁶

Subsequently, Vendiola reported the matter to PNP-ACG RACU 1,⁷ which determined that Vendiola had fallen victim to “vishing,”⁸ an offense proscribed under Section 9(s)⁹ of Republic Act No. 8484, or the Access Devices Regulation Act of 1998, as amended by Republic Act No. 11449.¹⁰

On June 13, 2023, PNP-ACG RACU 1 applied for a warrant to disclose computer data (WDCD)¹¹ for the violation of Section 9(s) of Republic Act No. 8484, as amended by Republic Act No. 11449, in relation to Section 6¹² of Republic Act No. 10175, or the Cybercrime Prevention Act of 2012 (Cybercrime Prevention Act).

⁶ *Id.* at 201–202.

⁷ *Id.* at 195–199.

⁸ *Id.* at 188.

⁹ Republic Act No. 8484 (1998), as amended by Republic Act No. 11449 (2019), sec. 9(s) states:
Sec. 9. *Prohibited Acts.*— The following acts shall constitute access device fraud and are hereby declared to be unlawful:

....
(s) accessing, with or without authority, any application, online banking account, credit card account, ATM account, debit card account, in a fraudulent manner, regardless of whether or not it will result in monetary loss to the account holder[.]

¹⁰ An Act Providing for Additional Prohibitions to and Increasing Penalties for Violations of Republic Act No. 8484, Otherwise Known as the “Access Devices Regulation Act of 1998” (2019).

¹¹ *Rollo*, pp. 200–205

¹² Cybercrime Prevention Act of 2012, sec. 6 states:

Sec. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies 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.

W

On June 21, 2023, the RTC granted the WDCD,¹³ thereby authorizing PNP-ACG RACU 1 to compel EWRB to release and preserve data/information related to account number 500023412872. The relevant portion of the WDCD reads:

WHEREFORE, by virtue of this WDCD, you are hereby AUTHORIZED to issue an order compelling EASTWEST RURAL BANK with office address at Beaufort, 5th Avenue corner 23rd Street, Bonifacio Global City, Taguig 1634 to release, preserve data/information pertaining **Eastwest Rural Bank Account Number 500023412872.**

With particular description of the data sought to be disclosed, to wit:

- a) Account information such as full name, personal information, and address of the Eastwest Rural bank account holder;
- b) Verification ID submitted when the account was opened;
- c) Contact details (email, Phone or cellular number[];) and
- d) Any other relevant information that will lead to the identity of the account holder/s and digital footprint.¹⁴ (Emphasis in the original)

Pursuant to the WDCD, PNP-ACG RACU 1 issued a Disclosure Order¹⁵ to EWRB.¹⁶

In response, EWRB filed an Entry of Appearance along with a Motion for Clarificatory Order¹⁷ with the RTC. In this Motion, EWRB requested clarification regarding the implications of the WDCD concerning Section 2¹⁸ of Republic Act No. 1405,¹⁹ also known as the Law on Secrecy of Bank Deposits (Bank Secrecy Law) and sought to have the Disclosure Order held in abeyance. Specifically, EWRB raised the following points: (1) the requested information was unrelated to any civil or criminal case pending before the court; (2) the Cybercrime Prevention Act did not repeal the Bank Secrecy Law, thus maintaining the prohibition against disclosing bank deposit information; and (3) A.M. No. 17-11-03-SC, also known as the Rule on Cybercrime Warrants, is

¹³ *Rollo*, pp. 98–99. The June 21, 2023 Warrant to Disclose Computer Data in WDCD No. 15-2023 was issued by Executive Judge Victor O. Concepcion of Branch 66, Regional Trial Court, San Fernando City, La Union.

¹⁴ *Id.* at 99.

¹⁵ *Id.* at 96–97.

¹⁶ *Id.* at 22–23.

¹⁷ *Id.* at 100–105.

¹⁸ Republic Act No. 1405 (1955), sec. 2 states:

Section 2. All deposits of whatever nature with banks or banking institutions in the Philippines including investments in bonds issued by the Government of the Philippines, its political subdivisions and its instrumentalities, are hereby considered as of an absolutely confidential nature and may not be examined, inquired or looked into by any person, government official, bureau or office, except upon written permission of the depositor, or in cases of impeachment, or upon order of a competent court in cases of bribery or dereliction of duty of public officials, or in cases where the money deposited or invested is the subject matter of the litigation.

¹⁹ An Act Prohibiting Disclosure of or Inquiry Into, Deposits with any Banking Institution and Providing Penalty Therefor (1955).

W

deemed inapplicable to EWRB because it did not meet the criteria to be classified as a service provider under the specified definition.²⁰

Ruling of the Regional Trial Court

In an Order²¹ dated July 3, 2023, the RTC denied EWRB's Motion, the dispositive portion of which states:

WHEREFORE, the *Motion for Clarificatory Order* filed by East West Banking Corporation is **DENIED** for lack of merit.

SO ORDERED.²² (Emphasis in the original)

The RTC concluded that the WDCD did not authorize law enforcement authorities to scrutinize the deposits of EWRB account number 500023412872. Furthermore, the WDCD did not mandate EWRB to divulge the account holder's deposits but focused on the identity of the account holder—full name, personal information, address, etc.—which fell within the scope of the Rule on Cybercrime Warrants. The RTC also noted that, once a criminal action was initiated, EWRB could file a motion to quash, and any related issues regarding the WDCD should be addressed by the court that subsequently acquired jurisdiction over the criminal case.²³

EWRB sought reconsideration, which the RTC denied in its Order²⁴ dated July 27, 2023.

EWRB thus filed a Petition for *Certiorari* with Application for Temporary Restraining Order (TRO) and/or Writ for Preliminary Injunction²⁵ before the CA, challenging the RTC's Orders dated July 3, 2023, and July 27, 2023.

Ruling of the Court of Appeals

In a Resolution²⁶ dated September 26, 2023, the CA dismissed EWRB's Petition for *Certiorari* due to three procedural deficiencies, specifically: (1) it failed to provide EWRB's address; (2) it did not include a clear and legible copy of Annex D as an attachment; and (3) it lacked the number and date of the Mandatory Continuing Legal Education (MCLE) compliance of the notary public involved. Additionally, the CA concluded that there was no grave abuse

²⁰ *Rollo*, pp. 101–104.

²¹ *Id.* at 107–108.

²² *Id.* at 108.

²³ *Id.* at 107–108.

²⁴ *Id.* at 118–119.

²⁵ *Id.* at 72–90.

²⁶ *Id.* at 8–11.

W

of discretion on the part of the RTC in issuing the WDCD and in its Orders dated July 3, 2023, and July 27, 2023.²⁷

The dispositive portion of the September 26, 2023 Resolution states:

PER CONSEQUENCE, the instant “Petition With Application for Temporary Restraining Order and/or Writ of Preliminary Injunction” filed by petitioner East West Rural Bank (EWRB) is **DISMISSED**.

....

SO ORDERED.²⁸ (Emphasis in the original)

EWRB’s Motion for Reconsideration²⁹ was also denied by the CA in its Resolution dated April 30, 2024.³⁰

Thus, EWRB filed the instant Petition for Review on *Certiorari*.³¹

Petitioner asserts that the RTC erred in issuing WDCDs under the Cybercrime Prevention Act, compelling banking institutions like EWRB to reveal depositor identities and information. Petitioner further contends that such disclosure violates the Bank Secrecy Law, as depositor identity is information protected by the Act’s confidentiality mandate. Moreover, it argues that the Cybercrime Prevention Act did not expressly repeal the Bank Secrecy Law; thus, disclosure of deposit information is impermissible absent established legal exemptions. Additionally, petitioner maintains that it is not a communication service provider and therefore falls outside the purview of the provisions of the Cybercrime Prevention Act authorizing WDCDs on bank deposits.³²

Regarding the procedural deficiencies cited by the CA, petitioner argues that its omission of its address, a clear and legible copy of a document, and the notary public’s MCLE number and compliance date, does not justify denying the Petition for *Certiorari*, invoking the established principle that litigation should be resolved on its merits rather than on technicalities.³³

In a Manifestation and Motion³⁴ dated November 4, 2024, the Office of the Solicitor General (OSG) asserts that the EWRB deposit account is protected under the Bank Secrecy Law, and consequently, the WDCD issued by the RTC against petitioner contravenes the provisions of the said law. Additionally, the OSG contends that the Cybercrime Prevention Act is inapplicable to petitioner,

²⁷ *Id.* at 9–10.

²⁸ *Id.* at 10–11.

²⁹ *Id.* at 59–67.

³⁰ *Id.* at 13–16.

³¹ *Id.* at 20–46.

³² *Id.* at 27–37.

³³ *Id.* at 37–43.

³⁴ *Id.* at 186–194.

W

as it does not meet the definition of a service provider under the Act. The OSG further clarifies that the EWRB account in question constitutes a bank deposit and does not solely involve computer data subject to disclosure under the law; thus, any information pertaining to the EWRB deposit account must remain confidential as mandated by the Bank Secrecy Law. Consequently, the EWRB deposit account cannot be disclosed pursuant to the WDCD or the Disclosure Order issued by respondent.³⁵

In light of these considerations, the OSG requested that the Court grant PNP-ACG RACU 1 a fresh period of 30 days from November 14, 2024, or until December 14, 2024, within which to file its Comment on the Petition.³⁶

On December 16, 2024, respondent submitted its Comment/Opposition³⁷ to the Petition. In its Comment, respondent argues that the WDCD issued by the RTC does not authorize the disclosure of financial transactions or deposit amounts, but rather pertains solely to information that could verify the identity and address of the account holder. In this context, it maintains that while the Bank Secrecy Law protects bank deposits as confidential information, the personal information of the account holder referenced in the WDCD may be disclosed pursuant to Section 14³⁸ of the Cybercrime Prevention Act and Section 4³⁹ of the Rule on Cybercrime Warrants.⁴⁰

Furthermore, respondent contends that petitioner falls within the scope of the Cybercrime Prevention Act, as it functions similarly to a service provider as defined in the Act. Through its online banking system, petitioner enables users to communicate via a computer system and retains subscriber information, which is a computer data under Section 3(e)⁴¹ of the Cybercrime Prevention Act. Accordingly, this information is subject to a disclosure warrant issued by the courts.⁴²

³⁵ *Id.* at 190–193.

³⁶ *Id.* at 193.

³⁷ *Id.* at 213–225.

³⁸ Cybercrime Prevention Act of 2012, sec. 14 states:

Sec. 14. *Disclosure of Computer Data.* — Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

³⁹ Disclosure of Computer Data.

⁴⁰ *Rollo*, pp. 217–218.

⁴¹ Cybercrime Prevention Act of 2012, sec. 3(e) states:

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

....

(e) *Computer data* refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages whether stored in local computer systems or online.

⁴² *Rollo*, pp. 222–223.

W

Issues

The following issues are presented for the Court's consideration:

1. Whether the procedural deficiencies noted by the CA in petitioner's Petition for *Certiorari* warrant its dismissal, or whether it should be considered on the merits.
2. Whether the Cybercrime Prevention Act implicitly repealed or superseded any provisions of the Bank Secrecy Law concerning the confidentiality of bank deposits.
3. Whether petitioner qualifies as a "service provider" under the Cybercrime Prevention Act, thereby subjecting it to the provisions of the Act authorizing the issuance of the WDCD.
4. Whether the WDCD issued by the RTC impermissibly infringes upon the confidentiality of bank deposits protected by the Bank Secrecy Law, or whether it permissibly seeks only the information necessary to verify the identity and address of the depositor or account holder.

Our Ruling

The Petition is partly meritorious.

*There was substantial compliance
with the formal requirements of a
petition for certiorari*

As discussed, the CA dismissed petitioner's Petition for *Certiorari* based on the following grounds: (1) it did not include petitioner's address; (2) it lacked a clear and legible copy of Annex D as an attachment; and (3) it did not provide the number and date of the MCLE compliance of the notary public involved.⁴³

Rule 46, Section 3,⁴⁴ in conjunction with Rule 65, Section 1,⁴⁵ of the Rules of Court mandates that a petition for *certiorari* include the actual addresses of

⁴³ *Id.* at 9–10.

⁴⁴ RULES OF COURT, Rule 46, sec. 3 states:

Sec. 3. *Contents and filing of petition; effect of noncompliance with requirements.* — The petition shall contain the full names and actual addresses of all the petitioners and respondents, a concise statement of the matters involved, the factual background of the case, and the grounds relied upon for the relief prayed for.

....

The failure of the petitioner to comply with any of the foregoing requirements shall be sufficient ground for the dismissal of the petition. (Citations omitted)

⁴⁵ RULES OF COURT, Rule 65, sec. 1 states:

Sec. 1. *Petition for certiorari.* ...

....

W

all petitioners and respondents. Non-compliance with this requirement constitutes a valid ground for dismissal.⁴⁶ However, the Court, in this instance, is inclined to overlook this technical defect, finding that petitioner has substantially complied with the rules. Although petitioner's address was not explicitly stated in the body of the Petition for *Certiorari*, the name and address of petitioner's counsel were clearly indicated. Furthermore, petitioner's address is ascertainable from the attached Special Power of Attorney and the certified true copy of the secretary's certificate.⁴⁷ Furthermore, petitioner promptly rectified this omission by filing a Motion for Reconsideration⁴⁸ accompanied by an Amended Petition for *Certiorari*.⁴⁹ Absent any showing of prejudice to the CA or respondent arising from this defect, the Court holds that petitioner substantially complied with the aforementioned rules.⁵⁰

The absence of a clear and legible copy of Annex D,⁵¹ which appears to be a photocopy of the WDCD issued by the RTC, raises the issue of whether the Petition for *Certiorari* is fatally defective. While petitions lacking essential pleadings and portions of the case record are generally subject to dismissal,⁵² the Court observes that the WDCD attached to the Petition for *Certiorari*, though less than ideal in clarity, remains legible. Moreover, petitioner has since rectified this deficiency by submitting a clearer copy⁵³ of the WDCD with its Motion for Reconsideration filed before the CA. It is well-established that petitions deficient in essential pleadings may nevertheless be allowed to proceed, or, if previously dismissed, be reinstated, upon subsequent submission of the required documents,⁵⁴ as in this case.

The CA also identified a defect in the Affidavit of Service of the Petition for *Certiorari* and the Verification and Certification of Non-Forum Shopping.⁵⁵ Specifically, Notary Public Atty. Irish L. Silverio-Aclan failed to include the number and date of her MCLE compliance. In this regard, it is a well-established principle that a lawyer's omission of the MCLE Compliance number and date in the pleadings will no longer result in the dismissal of the case.⁵⁶ To Our mind, this principle extends to the case at hand, considering that only the notary involved in notarizing the Affidavit and Verification failed to

The petition shall be accompanied by a certified true copy of the judgment, order or resolution subject thereof, copies of all pleadings and documents relevant and pertinent thereto, and a sworn certification of non-forum shopping as provided in the third paragraph of section 3, Rule 46.

⁴⁶ RULES OF COURT, Rule 46, sec. 3.

⁴⁷ *Rollo*, p. 38.

⁴⁸ *CA rollo*, pp. 78–90.

⁴⁹ *Id.* at 91–109.

⁵⁰ See *Duremdes v. Jorilla*, 871 Phil. 810, 820 (2020) [Per J. Inting, Second Division].

⁵¹ *CA rollo*, pp. 38–39.

⁵² *Duremdes v. Jorilla*, 871 Phil. 810, 822 (2020) [Per J. Inting, Second Division].

⁵³ *CA rollo*, pp. 110–111.

⁵⁴ *Duremdes v. Jorilla*, 871 Phil. 810, 820–821 (2020) [Per J. Inting, Second Division].

⁵⁵ *Rollo*, p. 42.

⁵⁶ *Malixi v. Baltazar*, 821 Phil. 423, 443 (2017) [Per J. Leonen, Third Division].

provide this information. In any event, petitioner subsequently supplied Atty. Silverio-Aclan's MCLE number and date in its Motion for Reconsideration.⁵⁷

In conclusion, the CA should have taken a more lenient stance on the technicalities mentioned above. In line with the Court's pronouncement in *Duremdes v. Jorilla*,⁵⁸ the CA should have recognized the submissions attached to petitioner's Motion for Reconsideration as substantial compliance with the formal requirements of Rule 65, Section 1 of the Rules of Court.

The foregoing notwithstanding, We concur with the conclusion of the CA that the RTC did not commit grave abuse of discretion in issuing the WDCD through its Orders dated July 3, 2023, and July 27, 2023. However, this Court recognizes that petitioner has raised novel issues concerning the confidentiality of bank deposits under Philippine law, specifically in relation to the Cybercrime Prevention Act, Republic Act No. 10173, or the Data Privacy Act of 2012, and the Rules on Cybercrime Warrants. Regrettably, the CA has not utilized the opportunity to address these matters comprehensively. Given the unprecedented nature of the issues presented, this Court deems it necessary to discuss and elaborate on them *seriatim* below.

*The Cybercrime Act did not repeal
the Bank Secrecy Law*

Petitioner relies heavily on the Bank Secrecy Law to challenge the validity of the WDCD. Specifically, Sections 2 and 3 of the law mandate that bank deposits are confidential and may only be disclosed under strictly defined circumstances, thus:

Section 2. **All deposits** of whatever nature with banks or banking institutions in the Philippines including investments in bonds issued by the Government of the Philippines, its political subdivisions and its instrumentalities, **are hereby considered as of an absolutely confidential nature** and may not be examined, inquired or looked into by any person, government official, bureau or office, except upon written permission of the depositor, or in cases of impeachment, or upon order of a competent court in cases of bribery or dereliction of duty of public officials, or in cases where the money deposited or invested is the subject matter of the litigation.

Section 3. It shall be **unlawful** for any official or employee of a banking institution to **disclose** to any person other than those mentioned in Section two hereof **any information concerning said deposits**. (Emphasis supplied)

⁵⁷ CA rollo, p. 112.

⁵⁸ 871 Phil. 810, 825 (2020) [Per J. Inting, Second Division].

W

In this regard, Section 2 of the Bank Secrecy Law declares these deposits absolutely confidential, prohibiting any examination, inquiry, or inspection by any person or entity unless specific exceptions are met. These exceptions include written permission from the depositor, impeachment proceedings, a court order issued in cases of bribery or dereliction of duty by public officials, or when the deposited funds are the subject matter of litigation. Section 3 further reinforces this confidentiality by making it illegal for bank officials or employees to disclose any deposit information to anyone not explicitly authorized by the law.

Conversely, respondent upholds the validity of the WDCD based on the provisions of the Cybercrime Prevention Act. This Act aims to penalize and prevent conduct that threatens the “confidentiality, integrity, and availability of information and data stored” in computer systems, networks, and databases. This includes “misuse, abuse, and illegal access” to such information. Essentially, the Act aims to protect data and information systems from a wide range of cyber threats, including unauthorized access, data breaches, and other forms of cyberattack that compromise the confidentiality, integrity, or availability of stored information.⁵⁹

While the Cybercrime Prevention Act emphasizes the protection of data confidentiality, it also recognizes that legitimate circumstances require information disclosure, providing a legal framework for such disclosures when justified and authorized by the courts, thus:

SEC. 12. *Real-Time Collection of Traffic Data.* — Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.

Traffic data refer only to the communication’s origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities.

All other data to be collected or seized or disclosed will require a court warrant.

Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.

The court warrant required under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed: (2) that there

⁵⁹ Cybercrime Prevention Act of 2012, sec. 2.

W

are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

....

SEC. 14. *Disclosure of Computer Data.* — Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation. (Emphasis supplied)

Generally, a court warrant is required for the collection, seizure, or disclosure of data pursuant to Section 12 of the Cybercrime Prevention Act. This warrant is issued only upon written application and examination under oath, demonstrating reasonable grounds to believe a cybercrime has been committed, is being committed, or is about to be committed; that the evidence sought is essential for conviction, solution, or prevention of such crimes; and that no other means of obtaining the evidence are readily available. Section 14 of the Act further clarifies the process for disclosing specific types of data. Law enforcement authorities, after obtaining a court warrant, may issue an order to any person or service provider to disclose or submit subscriber's information, traffic data, or other relevant data. This order must relate to a valid, docketed complaint under investigation, and the disclosure should be considered necessary and relevant for the purpose of investigating cybercrime offenses.⁶⁰

In this context, Section 6⁶¹ of the Cybercrime Prevention Act permits law enforcement authorities to collect or seize data for the purpose of conducting investigations related to crimes committed through information and communications technologies. Relevant to this case is the act perpetrated by Dela Cruz, which is punishable under the Access Devices Regulation Act of 1998, as amended. Specifically, Section 9(s) of the Act states:

Section 3. Section 9 of the same Act is hereby amended to read as follows:

Sec. 9. *Prohibited Acts.*— The following acts shall constitute access device fraud and are hereby declared to be unlawful:

....

⁶⁰ Cybercrime Prevention Act of 2012, secs. 12 and 14.

⁶¹ Cybercrime Prevention Act of 2012, sec. 6 states:

Sec. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act[.]

(s) accessing, with or without authority, any application, online banking account, credit card account, ATM account, debit card account, in a fraudulent manner, regardless of whether or not it will result in monetary loss to the account holder[.]

In light of these arguments, petitioner contends that the law must delineate specific exceptions for disclosing deposit information. Since the Cybercrime Prevention Act does not explicitly repeal any provisions of the Bank Secrecy Law, petitioner asserts that the Bank Secrecy Law should remain in effect, thereby prohibiting disclosure of any information concerning bank deposits.⁶²

In contrast, respondent argues that if there is any incompatibility between the Cybercrime Act of 2012 and the Bank Secrecy Law, the former, as a subsequent law, implicitly repeals the latter based on the repealing clause of the Cybercrime Act,⁶³ which states:

SEC. 30. *Repealing Clause.* — All laws, decrees or rules inconsistent with this Act are hereby repealed or modified accordingly. Section 33(a) of Republic Act No. 8792 or the “Electronic Commerce Act” is hereby modified accordingly.

Thus, respondent asserts that the WDCD, which mandates the disclosure of the identity of the EWRB account holder, is valid under the Cybercrime Prevention Act, irrespective of the provisions in the Bank Secrecy Law.⁶⁴

In *Chamber of Customs Brokers, Inc. v. Commissioner of Customs*,⁶⁵ We held that:

The question of whether a particular law has been repealed or not by a subsequent law is a matter of legislative intent. The lawmakers may expressly repeal a law by incorporating therein a repealing provision which expressly and specifically cites the particular law or laws, and portions thereof, that are intended to be repealed. A declaration in a statute, usually in its repealing clause, that a particular and specific law, identified by its number or title, is repealed is an express repeal; all others are implied repeals.⁶⁶ (Citations omitted)

Given the foregoing, the Court holds that the Bank Secrecy Law was not revoked, withdrawn or repealed—expressly or impliedly—by Congress with the enactment of the Cybercrime Prevention Act.

Notably, had Congress intended to withdraw or revoke the confidentiality of deposits under the Bank Secrecy Law, it would have explicitly mentioned Sections 2 and 3 of the law, in the same way that it specifically mentioned

⁶² *Rollo*, pp. 31–34.

⁶³ *Id.* at 222.

⁶⁴ *Id.* at 224.

⁶⁵ 936 Phil. 372 (2023) [Per J. Kho, Jr., Second Division].

⁶⁶ *Id.* at 381.

Section 33(a) of Republic Act No. 8792, as among the laws repealed by the Cybercrime Prevention Act.

The Court also holds that the Cybercrime Prevention Act could not have impliedly repealed the Bank Secrecy Law. In *Commissioner of Internal Revenue v. Semirara Mining Corp.*,⁶⁷ citing *Mecano v. Commission on Audit*,⁶⁸ the Court extensively discussed how repeals by implication operate, to wit:

There are two categories of repeal by implication. The first is where provisions in the two acts on the same subject matter are in an irreconcilable conflict. The later act to the extent of the conflict constitutes an implied repeal of the earlier one. The second is if the later act covers the whole subject of the earlier one and is clearly intended as a substitute, it will operate to repeal the earlier law.

Implied repeal by irreconcilable inconsistency takes place when the two statutes cover the same subject matter; they are so clearly inconsistent and incompatible with each other that they cannot be reconciled or harmonized; and both cannot be given effect, that is, that one law cannot [be] enforced without nullifying the other.⁶⁹ (Citation omitted)

In other words, implied repeal occurs in two scenarios: (1) irreconcilable conflict between provisions of the two acts on the same subject matter; and (2) when the later act covers the entire subject of the earlier act and is intended as a substitute. Neither kind of implied repeal exists in this case.

First, there is no irreconcilable conflict. Implied repeal by inconsistency requires that the two statutes cover the same subject matter and be so incompatible that they cannot be harmonized. While both laws touch upon data or information and their disclosure as may be permitted by law, they do not cover precisely the same subject matter. The Bank Secrecy Law specifically focuses on confidentiality of bank deposit information. The Cybercrime Prevention Act, on the other hand, deals with a broader range of data related to cybercrime, including computer data, subscriber's information, traffic data and non-content data. Evidently, these are distinct categories. Therefore, the necessary element of same subject matter and irreconcilable conflict for implied repeal is absent.

Second, the Cybercrime Prevention Act does not cover the entire subject of the Bank Secrecy Law and is not intended as a substitute thereof. The Bank Secrecy Law's focus is on bank deposits. The scope of the Cybercrime Prevention Act is far broader, encompassing various cybercrime offenses and disclosure of related data. It is clearly not intended to replace the Bank Secrecy

⁶⁷ 811 Phil. 113, 123 (2017) [Per J. Caguioa, First Division].

⁶⁸ 290-A Phil. 272, 280-281 (1992) [Per J. Campos, Jr. *En Banc*].

⁶⁹ *Commissioner of Internal Revenue v. Semirara Mining Corp.*, 811 Phil. 113, 123 [Per J. Caguioa, First Division].

Law's specific provisions regarding bank deposit confidentiality. Thus, neither of the recognized grounds for implied repeal exists in this case.

It bears noting at this point that, contrary to the petitioner's assertions, the provisions of the Cybercrime Prevention Act regarding the disclosure of subscriber information or identity can be enforced without undermining the specific protections for bank deposit information provided by the Bank Secrecy Law. As will be detailed below, the WDCD's authority to disclose the identity of the EWRB account holder must be examined not only through the lens of the Bank Secrecy Law but also in the context of the Cybercrime Prevention Act, which permits information disclosure under specified circumstances.

However, antecedent to this matter, it behooves the Court to ascertain whether petitioner, as a financial institution, is subject to the provisions of the Cybercrime Prevention Act and its attendant Rules on Cybercrime Warrants. This determination is critical, as these rules impose a duty upon covered entities to cooperate and assist law enforcement authorities in the collection and recording of information delineated in WDCDs.

Petitioner qualifies as a "service provider" under the Cybercrime Prevention Act

The Cybercrime Prevention Act defines "service provider" as: "(1) [a]ny public or private entity that provides to users of its service the ability to communicate by means of a computer system; and (2) [a]ny other entity that processes or stores computer data on behalf of such communication service or users of such service."⁷⁰

Service providers bear specific duties and responsibilities toward law enforcement authorities. Specifically, service providers are obligated, among others, to cooperate and assist law enforcement in the collection and recording of various types of data, including traffic data, subscriber information, content data, and computer data.⁷¹ This assistance may involve technical support or system access, but it is contingent upon the existence of a lawful order, particularly a court warrant.⁷² Accordingly, upon the issuance of a court warrant, law enforcement authorities may compel service providers to disclose or submit pertinent computer data within their custody or control.⁷³ They are also bound to comply with such order within 72 hours of receipt.⁷⁴ Furthermore,

⁷⁰ Cybercrime Prevention Act of 2012, sec. 3(n).

⁷¹ Cybercrime Prevention Act of 2012, sec. 12.

⁷² Cybercrime Prevention Act of 2012, secs. 12 and 14.

⁷³ Cybercrime Prevention Act of 2012, sec. 14.

⁷⁴ Cybercrime Prevention Act of 2012, sec. 14.

service providers are required to preserve data as directed by law enforcement with varying preservation periods depending on the data type and the status of legal proceedings.⁷⁵

Parenthetically, the Rule on Cybercrime Warrants sets forth the procedure for the application and grant of warrants and related orders involving the preservation, disclosure, interception, search, seizure, and/or examination, as well as the custody, and destruction of computer data under the Cybercrime Prevention Act.⁷⁶

In light of the foregoing recitals, petitioner contends that it does not fall within the definition of a “service provider” under the Cybercrime Prevention Act, its implementing rules, and the Rule on Cybercrime Warrants. Specifically, petitioner argues that the Act’s definition pertains exclusively to entities providing communication services or those processing data on behalf of such service providers. Given that petitioner’s primary business is providing financial services rather than communication services, it asserts that it is not subject to the aforementioned provisions.⁷⁷

We disagree.

The language employed in the Cybercrime Prevention Act, specifically the phrase “any public or private entity,”⁷⁸ reflects a legislative intent to encompass a diverse array of entities, extending beyond those primarily engaged in providing communication services. This interpretation is underscored by the fundamental principle of statutory construction, which holds that “where the words of a statute are clear, plain, and free from ambiguity, they must be given their literal meaning and applied without attempted interpretation.”⁷⁹ Furthermore, it is a basic tenet of statutory construction that “where the law does not distinguish, the courts should not distinguish. *Ubi lex non distinguit nec nos distinguere debemos.*”⁸⁰ In this context, the courts are compelled to interpret the law strictly according to its written provisions, without imposing distinctions not explicitly stated therein.

In light of these considerations, the Court holds that petitioner qualifies as a service provider under the broad definition outlined in the Cybercrime Prevention Act.

⁷⁵ Cybercrime Prevention Act of 2012, sec. 13.

⁷⁶ CYBERCRIME WARRANTS RULE, sec. 1.2.

⁷⁷ *Rollo*, pp. 34–37.

⁷⁸ Cybercrime Prevention Act of 2012, sec. 3(n).

⁷⁹ *Secretary Soliman v. Santos*, 944 Phil. 448, 459 (2023) [Per J. Marquez, First Division].

⁸⁰ *Ambrose v. Suque-Ambrose*, 905 Phil. 149, 155 (2021) [Per J. Gaerlan, First Division].

W

We now turn to examine how petitioner's activities align with the statutory definition of a "service provider."

Petitioner's operational activities related to its banking or financial services demonstrate that it falls within the ambit of service providers as defined under the Cybercrime Prevention Act. Modern banking practices, which petitioner undoubtedly employs, rely heavily on computer systems to facilitate customer communication.⁸¹ This is evident in petitioner's array of digital services, including online banking platforms, mobile applications, and automated email notifications. Through these digital platforms, petitioner effectively provides its customers communication channels for various financial activities and customer service operations. This capability clearly demonstrates its role as a service provider.⁸² Importantly, while communication may not be petitioner's primary function, the Court recognizes that the mere fact that it offers these communicative capabilities through computer systems substantially fulfills the Act's criteria for a "service provider."

Moreover, as a banking institution, petitioner undeniably processes and stores substantial amounts of computer data, both for its own operations and for its customers. This data includes account balances, transaction histories, and personal information of its customers. To Our mind, this processing and storage of data are considered to be "on behalf of . . . users of such service,"⁸³ referring to petitioner's customers. Given that petitioner, by virtue of its function as a banking institution, processes and stores significant volumes of computerized data—both in its operational capacity and on behalf of its customers—it clearly meets the statutory definition of "service provider."

Consequently, petitioner, by virtue of its communication services and data management practices, clearly qualifies as a "service provider" under the Cybercrime Prevention Act. As such, petitioner is bound by the provisions of the Act, particularly those relating to data disclosure as stipulated in Section 14.

*The WDCD and Disclosure Order
for account holder verification
information is permissible under
current state of laws and does not
violate bank secrecy provisions*

The Bank Secrecy Law does not provide a specific definition of "deposit." In this regard, the law states:

Section 2. All deposits of whatever nature with banks or banking institutions in the Philippines. . . are hereby considered as of an absolutely

⁸¹ See Republic Act No. 12010 (2024), Anti-Financial Account Scamming Act (AFASA); *rollo*, pp. 222–223.

⁸² See *rollo*, pp. 222–223.

⁸³ Cybercrime Prevention Act of 2012, sec. 3(n).

W

confidential nature and may not be examined, inquired or looked into by any person, government official, bureau or office. . .

Section 3. It shall be unlawful for any official or employee of a banking institution to disclose to any person other than those mentioned in Section two hereof any information concerning said deposits.

Petitioner argues that the Bank Secrecy Law's provision that "any information" concerning deposits is confidential imposes a blanket prohibition against disclosing information, particularly the specifics sought under the WDCD. This includes: (1) account details such as the account holder's full name, personal information, and address; (2) the verification ID submitted at account opening; (3) contact information, including email and phone numbers; and (4) any other relevant details that could reveal the identity of the account holder and their digital footprint.⁸⁴

According to petitioner, the confidentiality mandated by the Bank Secrecy Law extends beyond the financial contents of the deposit account to include all details pertaining to the identity of the account holder. The explicit reference to "any information" in the law supports this assertion and highlights the prohibition against disclosing information related to bank deposits.⁸⁵

Conversely, respondent argues that while the Bank Secrecy Law generally protects the confidentiality of bank deposits, it permits the disclosure of personal information and other details specified in the WDCD. Respondent relies on Section 14⁸⁶ of the Cybercrime Prevention Act and Section 4⁸⁷ of the Rule on Cybercrime Warrants, both of which authorize the disclosure of subscriber information under specific circumstances. In this context, respondent asserts that the term "subscribers" refers to the customers of petitioner who hold accounts and utilize petitioner's services.⁸⁸

In light of these considerations, the Court concludes that the provisions of the Cybercrime Prevention Act concerning the disclosure of subscriber information or identity can be applied without undermining the confidentiality of bank deposit information afforded by the Bank Secrecy Law.

The Court references Republic Act No. 3591,⁸⁹ Section 3(f), which defines deposit as:

⁸⁴ *Rollo*, p. 99.

⁸⁵ *Id.* at 28–29.

⁸⁶ Cybercrime Prevention Act of 2012, sec. 14 states:

Sec. 14. *Disclosure of Computer Data.* — Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

⁸⁷ *Disclosure of Computer Data.*

⁸⁸ *Rollo*, p. 223.

⁸⁹ Republic Act No. 3591 (1963), An Act Establishing the Philippine Deposit Insurance Corporation, Defining its Powers and Duties and for Other Purposes.

the unpaid balance of money or its equivalent received by a bank in the usual course of business and for which it has given or is obliged to give credit to a commercial, checking, savings, time or thrift account, or which is evidenced by its certificate of deposit, ... [or other evidence of deposit issued in accordance with Bangko Sentral ng Pilipinas rules and regulations and other applicable laws. . .]⁹⁰

From this definition, it can be inferred that confidentiality associated with deposits primarily safeguards their financial details as opposed to basic identifying information. This interpretation aligns with the legislative intent of the Bank Secrecy Law, which was enacted to promote public investment in government securities and bank deposits during a period when the country required substantial capital and credit facilities for post-World War II economic revitalization.⁹¹ Thus, the primary aim of the Bank Secrecy Law is to protect the depositor's financial transaction, allowing for disclosure only under specified conditions.

While the Bank Secrecy Law encompasses a broad array of information requiring protection and confidentiality, existing laws have established exceptions to this general rule, particularly regarding identifying information associated with deposits. In this regard, the Cybercrime Prevention Act specifically delineates subscriber information, defined as follows:

(o) *Subscriber's information* refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which identity can be established:

- (1) The type of communication service used, the technical provisions taken thereto and the period of service;
- (2) The subscriber's identity, postal or geographic address, telephone and other access numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; and
- (3) Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

On this point, the Court agrees with respondent that the customers of petitioner who hold accounts and utilize petitioner's services are considered as subscribers under the Cybercrime Prevention Act. As such, information falling within the scope of the above definition may be legally disclosed to law

⁹⁰ Republic Act No. 3591, sec. 3(f) in relation to Bangko Sentral ng Pilipinas, A LEGAL PRIMER: THE LAWS ON SECRECY OF BANK DEPOSITS, Bangko Sentral ng Pilipinas (2024), at 4, available at https://www.bsp.gov.ph/Media_and_Research/Primers%20Faqs/Primer_on_Bank_Secrecy.pdf (last accessed June 23, 2024).

⁹¹ Bangko Sentral ng Pilipinas, A LEGAL PRIMER: THE LAWS ON SECRECY OF BANK DEPOSITS, Bangko Sentral ng Pilipinas (2024), at 1., available at https://www.bsp.gov.ph/Media_and_Research/Primers%20Faqs/Primer_on_Bank_Secrecy.pdf (last accessed June 23, 2024).

enforcement authorities under specified circumstances, without necessarily violating the confidentiality of bank deposits.

Ultimately, the Court determines that while the Bank Secrecy Law mandates protection of the financial details of deposits, it does not prevent the disclosure of basic identifying information in accordance with the provisions of the Cybercrime Prevention Act. This interpretation allows for a balanced approach to privacy rights and the need for disclosures, as may be allowed by law, facilitating compliance with both statutes in a manner that upholds the intent behind the Bank Secrecy Law while allowing necessary transparency in cases governed by the Cybercrime Prevention Act, particularly in the prosecution of cyber-related offenses such as hacking, identity theft, cybersex, child pornography, and online libel.

In fact, various laws have carved out exceptions to the general rule concerning the confidentiality of bank deposits, thereby permitting information related to these deposits to be examined, inquired into, or scrutinized.⁹²

For instance, Republic Act No. 9160, also known as the Anti-Money Laundering Act of 2001 (AMLA), empowers the Anti-Money Laundering Council (AMLC) to investigate bank deposits linked to unlawful activities or money laundering offenses. The AMLC can examine these deposits with a court order based on probable cause or without a court order concerning predicate crimes such as kidnapping, drug violations, hijacking, arson, murder, and terrorism.⁹³ Additionally, the AMLC has the authority to investigate suspicious transactions, money laundering, and terrorism financing activities.⁹⁴

Similarly, Republic Act No. 11479, or the Anti-Terrorism Act of 2020 (Anti-Terrorism Act), authorizes the AMLC to investigate upon issuance of a preliminary court order of proscription or designation, investigating: (a) any property or funds related to terrorism financing or violations of the Anti-Terrorism Act; and (b) property or funds of individuals suspected of facilitating offenses under the Act. In these cases, the AMLC can examine deposits and investments with any bank or non-bank financial institution without a court order.⁹⁵

Just as the aforementioned laws create exceptions to bank deposit confidentiality, the Cybercrime Prevention Act provides a legal basis for limited disclosure of information concerning the identity of the depositor or account holder. Similar to the aforementioned laws, disclosures may occur even during

⁹² Bangko Sentral ng Pilipinas, *supra* note 91, at 7–18.

⁹³ Anti-Money Laundering Act of 2001, secs. 3(i), 4, and 7; Bangko Sentral ng Pilipinas, *supra* note 91, at 9–10.

⁹⁴ Bangko Sentral ng Pilipinas, Implementing Rules and Regulations of the Anti-Money Laundering Act of 2001, as amended, Republic Act. No. 9160, Rule 6, sec. 1.9.1. (2018); Bangko Sentral ng Pilipinas, *supra* note 91, at 9–10.

⁹⁵ Anti-Terrorism Act of 2020, secs. 4, 6, 7, 10–12; Bangko Sentral ng Pilipinas, *supra* note 91, at 13.

the investigation stage and even when no case is pending before a court of competent jurisdiction. Specifically, if there is an investigation regarding acts constituting cybercrime offenses, law enforcement authorities are legally authorized to access relevant information held by service providers, akin to the powers granted under the AMLA and the Anti-Terrorism Act, which similarly allow for access to financial information in the pursuit of criminal investigations.

The Court recognizes that both the AMLA and the Anti-Terrorism Act explicitly allow for the examination of bank deposits and related information under specific circumstances. Conversely, the language of the Cybercrime Prevention Act appears broader in scope and does not explicitly identify bank deposits as falling within the ambit of information subject of the WDCD. Petitioner appears to argue that this distinction supports its assertion that the Cybercrime Prevention Act should not be construed as an exception to the Bank Secrecy Law with respect to the confidentiality of bank deposits.⁹⁶ The Court, however, disagrees. Although the Cybercrime Prevention Act does not specifically mention banks or deposits, it may nonetheless be interpreted as an exception to the confidentiality of bank deposits because, as discussed above, banks function as service providers and their customers are regarded as subscribers.

To further illustrate this point, We draw an analogy to Republic Act No. 10173, known as the Data Privacy Act of 2012,⁹⁷ which establishes criteria for the lawful processing of personal information of data subjects⁹⁸ by personal information controllers.⁹⁹ In this regard, the relevant provisions thereof are as follows:

SEC. 12. *Criteria for Lawful Processing of Personal Information.* – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

....

⁹⁶ *Rollo*, p. 32

⁹⁷ *Id.* at 222–223.

⁹⁸ Data Privacy Act of 2012, sec. 3(h) states:

SEC. 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

....

(h) *Personal information controller* refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

(1) A person or organization who performs such functions as instructed by another person or organization; and

(2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

⁹⁹ Data Privacy Act of 2012, sec. 3(c) states:

....

(c) *Data subject* refers to an individual whose personal information is processed.

(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

....

(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

SEC. 13. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

....

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

In light of the provisions of the Data Privacy Act, the National Privacy Commission (NPC) issued Privacy Policy Office Advisory Opinion No. 2021-026. This advisory addresses the disclosure of personal information of *data subjects*, including names, addresses, delivery addresses, email addresses, and mobile or other contact numbers, by *personal information controllers* such as online merchants, financial institutions, and *banks* for the purpose of fraud investigations. The NPC asserts that such disclosure is permitted under Section 12(f) of the Data Privacy Act. Additionally, the NPC contends that the sharing of this information with law enforcement and regulatory agencies may be justified under Section 12(c) of the Data Privacy Act, which pertains to processing necessary for compliance with a legal obligation, and/or Section 12(e), which addresses processing required to fulfill functions of public authority, thereby encompassing the processing of personal data essential to the fulfillment of its mandate.¹⁰⁰ Consequently, under the Data Privacy Act, banks are considered personal information controllers, and their customers are data subjects.¹⁰¹

In response to these considerations, the Bangko Sentral ng Pilipinas (BSP), through the Office of the Deputy Governor for Financial Supervision Sector, issued Memorandum No. M-2021-059. This memorandum specifically advises all BSP Supervised Financial Institutions (BSFIs), which evidently includes

¹⁰⁰ NPC Opinion No. 2021-026 (2021); *rollo*, pp. 218–219.

¹⁰¹ See BSP Memorandum No. M-2021-059 (2021); *rollo*, p. 218.

herein petitioner, to cooperate and share relevant information with third parties, including law enforcement agencies, in the conduct of fraud investigations. The BSP outlines the types of information that may be disclosed, which encompass the data subject's name, address, email address, mobile or other contact details, as well as bank and financial account information, and bank or financial transaction details. Furthermore, the memorandum emphasizes that BSFIs must adhere to fundamental data privacy principles of transparency, legitimate purpose, and proportionality. Importantly, it also clarifies that an existing court order or proceeding is not a prerequisite for such information sharing to take place.¹⁰²

Although these administrative issuances or guidelines are not binding on the Court, they provide valuable insight into the permissibility of disclosing basic identifying information concerning bank deposits under the Data Privacy Act, despite the absence of explicit mention of the term "banks" and "bank deposits," which mirrors the broader provisions within the Cybercrime Prevention Act. Moreover, it is important to highlight that the BSP explicitly permits the disclosure of basic identifying information related to bank deposits, consistent with information stated in the WDCD.¹⁰³ This stands in contrast to the petitioner's assertions, which suggest otherwise.

In conclusion, the interplay between the Cybercrime Prevention Act, the Data Privacy Act, and related administrative guidelines suggests a legal framework wherein certain exceptions to bank deposit confidentiality are recognized. The Court's analysis confirms that, notwithstanding petitioner's assertions, there is a legitimate legal basis for the disclosure of basic identifying information as outlined in the WDCD, provided that the safeguards delineated in the Cybercrime Prevention Act are observed.

At this point, the Court also considers Republic Act No. 12010, or the Anti-Financial Account Scamming Act (AFASA). "The AFASA seeks to combat financial cybercrimes, safeguard the interests of financial consumers, and uphold the integrity of the financial system."¹⁰⁴ Section 4(b)¹⁰⁵ specifically

¹⁰² *Id.*

¹⁰³ *Id.*

¹⁰⁴ *Bangko Sentral ng Pilipinas, supra* note 91, at 3.

¹⁰⁵ AFASA, sec. 4 states:

Sec. 4. *Prohibited Acts.* - The following acts shall constitute Financial Account scamming under this Act:

(b) *Social Engineering Schemes.* - A social engineering scheme is committed by a person who obtains sensitive identifying information of another person, through deception or fraud, resulting in unauthorized access and control over the person's Financial Account, by performing any of the following acts:

(1) Misrepresenting oneself as acting on behalf of an Institution, or making false representations to solicit another person's sensitive identifying information; or
(2) Using electronic communications to obtain another person's sensitive identifying information. (Emphasis supplied)

W

criminalizes “social engineering schemes,” defined as obtaining sensitive identifying information through deception or fraud to gain unauthorized access to a financial account. This includes misrepresenting oneself as an institution or using electronic communication for this purpose.

Significantly, AFASA grants the BSP the authority to investigate financial accounts and share relevant information with law enforcement and other competent authorities, subject to the Act’s limitations.¹⁰⁶ For this purpose, Section 13¹⁰⁷ of the AFASA grants the BSP or its authorized officers the authority to apply for cybercrime warrants and issue related orders under the Cybercrime Prevention Act. This authority is conferred without prejudice to the existing powers of the cybercrime units of the National Bureau of Investigation (NBI) and the Philippine National Police (PNP). Additionally, the BSP may seek assistance from the NBI and PNP in investigating cases and enforcing cybercrime warrants pertaining to violations of this Act.

Consequently, the relevant provisions of laws containing prohibitions against inquiry into or disclosure of deposits, including the Bank Secrecy Law, shall not apply to financial accounts, encompassing both interest-bearing and non-interest-bearing deposits, that are under investigation by the BSP.¹⁰⁸

In light of the preceding discussion regarding relevant legislation, the Court finds that current state of laws, encompassing the Cybercrime Prevention Act, the Data Privacy Act, and the AFASA, explicitly permits the disclosure of information related to bank deposits in investigations of cybercrimes, such as those presented in this case.

Accordingly, given the foregoing premises, the Court finds the WDCD and the resulting Disclosure Order valid.

The Cybercrime Prevention Act explicitly permits the disclosure of information under defined circumstances. The Act establishes the following requisites for permissible information disclosure: (1) a court warrant issued upon a written application demonstrating reasonable grounds to believe that any of the crimes enumerated in the Act has been, is being, or is about to be committed, that the evidence to be obtained is essential to the conviction of any

¹⁰⁶ AFASA, secs. 13–15.

¹⁰⁷ AFASA, sec. 13 states:

Sec. 13. *Cybercrime Warrants and Related Orders.* - Without prejudice to the authority of the cybercrime units of the National Bureau of Investigation (NBI) and the Philippine National Police (PNP), the BSP or its duly authorized officer or body shall have the authority to apply for cybercrime warrants and to issue the orders provided in Chapter IV of Republic Act No. 10175, or the "Cybercrime Prevention Act of 2012", with respect to the electromagnetic communications used in any violation of this Act. The BSP may request the assistance of the NBI and the PNP in the investigation of cases and the enforcement and implementation of cybercrime warrants and related orders for violations of this Act.

¹⁰⁸ AFASA, sec. 12; *Bangko Sentral ng Pilipinas*, *supra* note 91, at 3.

person for, or to the solution of, or to the prevention of, any such crimes, and that there are no other means readily available for obtaining such evidence;¹⁰⁹ (2) the existence of a valid complaint officially docketed and assigned for investigation, where the disclosure is demonstrably necessary and relevant to the investigation;¹¹⁰ and (3) prior authorization by a court through a WDCD, strictly limiting the disclosed information to that specifically permitted under the Cybercrime Prevention Act, namely subscriber information and relevant traffic data held by the service provider.¹¹¹

The Court finds that the requisites for lawful disclosure under the Cybercrime Prevention Act are satisfied. The application for a WDCD, filed by respondent on June 13, 2023, sought information pertinent to a violation of Section 9(s) of Republic Act No. 8484, as amended, in relation to Section 6 of the Cybercrime Prevention Act. The investigation into unauthorized transactions required the disclosure of specific account information—including the full name, personal information, address, verification ID, and contact details of the account holder—to effectively identify the perpetrator and trace their digital footprint. This information was demonstrably necessary and relevant, as the existing information (account number only) was insufficient for a complete investigation under Republic Act No. 8484, as amended. Finally, the RTC's issuance of the WDCD, and the subsequent Disclosure Order by the respondent, both strictly limited the disclosed information to that explicitly permitted under the Cybercrime Prevention Act. Consequently, the requisites for lawful disclosure are satisfied, and the WDCD and resulting Disclosure Order are valid.

While bank secrecy constitutes a statutory right accorded under the Bank Secrecy Law, the mandate imposed by WDCD and Disclosure Order requiring the disclosure of the identity of the EWRB account holder must be examined not only through the lens of the Bank Secrecy Law but also in the context of the Cybercrime Prevention Act, which permits disclosure of information under defined conditions. A strictly literal interpretation of the Bank Secrecy Law would undermine the stated objectives of the Cybercrime Prevention Act and the recently enacted AFASA, potentially hindering the prosecution of cyber-related crimes. Moreover, such an inflexible approach could inadvertently impede the effective prosecution and adjudication of crimes contemplated under these statutes, solely on the basis that “any” information pertaining to deposits is deemed confidential.

ACCORDINGLY, the Petition is **DENIED**. The Resolutions dated September 26, 2023, and April 30, 2024, of the Court of Appeals in CA G.R. SP. No. 180524 are **AFFIRMED**.

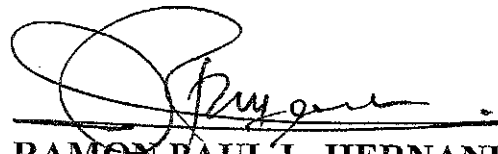
¹⁰⁹ Cybercrime Prevention Act of 2012, sec. 12.

¹¹⁰ Cybercrime Prevention Act of 2012, sec. 14.

¹¹¹ Cybercrime Prevention Act of 2012, secs. 12 and 14.

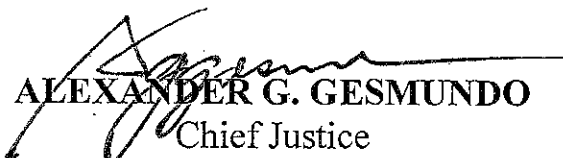
W

SO ORDERED.

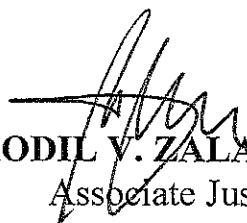


RAMON PAUL L. HERNANDO
Associate Justice
Working Chairperson

WE CONCUR:



ALEXANDER G. GESMUNDO
Chief Justice
Chairperson



RODIL V. ZALAMEDA
Associate Justice



RICARDO R. ROSARIO
Associate Justice

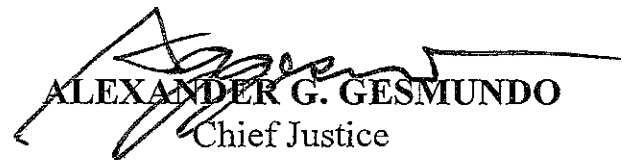


JOSE MIDAS P. MARQUEZ
Associate Justice

W

CERTIFICATION

Pursuant to Article VIII, Section 13 of the Constitution, I certify that the conclusions in the above Decision had been reached in consultation before the case was assigned to the writer of the opinion of the Court's Division.



ALEXANDER G. GESMUNDO
Chief Justice