BETWEEN

Hajah Siti Fatimah Binti Abdullah @ Ling Yen Ling	**1st Plaintiff**
Haji Mazlan Bin Hj Abd Samad	**2nd Plaintiff**
Aisah Binti Ahmat	**3rd Plaintiff**
Muhammad Hayattuddin Bin Mohammad Jaylani	**4th Plaintiff**
Mohammad Ma'aruf Izzuddin@Danial Bin Mohammad Jaynudden	**5th Plaintiff**

AND

BANK ISLAM BRUNEI DARUSSALAM BERHAD	**Defendant**

(Intermediate Court If Brunei Darussalam)
(Civil Suit/COM 54 of 2022)

Pg Masni Pg Hj Bahar, Judge.
Date of Judgment: 19th January, 2026.

Headnote: Banking- Negligence- Breach to safe guard the customer's credential- Mobile App Transaction - Duty of care to provide secure banking services- Contractual Clause to exclude Liability.

Mr Harif Ibrahim (M/S LT COL (RTD) Harif Ibrahim) from the Plaintiffs.
Mr Kamal Shari and Ms Lim Li Chyi (M/S Yusof Halim & Partners) for the Defendant.

Case cited:
Brown v Dunn (1893) 6 R 67 (HL)

JUDGMENT

Pg Masni, Judge:

Introduction:

1. The Plaintiffs bring an action against BIBD for negligence and breach of duty of care arising from a series of unauthorised online banking transactions that resulted in losses totaling approximately BND160,000 from their BIBD accounts.

Background:

2. This claim concerns transactions carried out between the 18th and the 22nd of May 2023, during which the Plaintiffs jointly held Perdana accounts were unlawfully accessed and depleted through multiple transfers to third-party accounts within BIBD's own system. BIBD Bank were promptly notified. BIBD later discovered that the transactions were processed internally and transferred to a third party.

3. Plaintiffs alleged that the losses were not attributed by any of fault, negligence, or misuse but rather by serious and systemic failures within BIBD's mobile banking and fraud detection systems.

4. Hence, the Plaintiffs' claim that BIBD owed the Plaintiffs a duty of care to safeguard their accounts. Plaintiffs claimed that BIBD had breached this duty and was negligent in failing to maintain a secure banking system, protect the Plaintiffs' funds and information, prevent third-party access, and alert the Plaintiffs of the unauthorized transactions. As a result, the Plaintiffs suffered losses and damages. And the Plaintiffs are now claiming full payment of the sum BND$168,549.00, which was amended during the hearing to BND$ 160,000 due to an oversight.

5. The Defendant, BIBD, denied liability and blamed the 1st Plaintiff for voluntarily revealing confidential Banking information to a third party such as valid login credentials and OTPs and failed to safeguard her credentials.

6. The Bank further relied on general fraud awareness messages and compliance with internal security protocols as a basis for denying negligence, which the 1st Plaintiff had ignored.

7. Both the 1st and the 2nd Plaintiffs consistently denied authorising any of the disputed transactions or knowingly disclosing sensitive credentials such as OTPs, PINs, or passwords.

Plaintiffs' case:

8. Hjh Siti Fatimah Binti Abdullah @ Ling Yen Ling (PW1) is the 1st Plaintiff named in this suit and Haji Mazlan bin Hj Abd Samad is the 2nd Plaintiff named in this suit. Both the 1st and the 2nd Plaintiffs gave evidence in Court.

9. The 1st Plaintiff will be referred to as PW1 and the 2nd Plaintiff will be referred to as PW2.

10. PW1 affirmed an affidavit dated the 28th April 2025 affirming that she has been authorized by the 3rd, 4th and the 5th Plaintiff to make the said affidavit and to testify in court on their

behalf. She also affirmed that the 2nd Plaintiff, Haji Mazlan bin Haji Abd Samad, is her husband.

11. In my judgement, I will only summarise what is pertinent, including the evidence given in cross-examination and re-examination.

PW1: Hjh Siti Fatimah Binti Abdullah @ Ling Yen Ling

12. PW1 testified that she had been a member of the BIBD Perdana Banking service for approximately six to seven years, during which she dealt with two Relationship Managers (RM): Dk Vivi and Md Khairuddin bin Hj Musa, the latter being the officer who assisted her during the incident.

13. She admitted that she is the primary manager of several joint accounts held with her family members, who are her husband (PW2), her mother (PW3), her nephew (PW4), and her son (PW5).

14. She informed the court that she and PW2 opened the following bank account on the 11th July 2020.

    a. Perdana Account no: 00-001-02-0038917, joint account;

    b. Perdana Account: 00-001-02-1160720, joint account;

    c. Perdana Account: 00-020-02-0018361, under PW1's name.

15. Following that she opened a saving account and joint account with the following:

    a. Saving Account no: 00-001-02-0748157, joint account with 4th Plaintiff;

    b. Saving Account no: 00-010-02-0124726, joint account with 3rd Plaintiff;

    c. Joint Account no: 00-001-02-1365484, joint account with 5th Plaintiff.

16. Being the primary manager of their account, PW1 admitted that she had registered all the six (6) accounts under her personal Mobile Banking Application for her to have exclusive access and to transact both personal and joint accounts remotely from her mobile phone. She admitted that the other Plaintiff has no operational involvement.

BIBD Mobile Banking Application (The said App).

17. The BIBD Mobile Application, referred to as the said App, functions as a Nexgen Wallet platform which enable PW1 to conduct transactions seamlessly and remotely. By using this service, PW1 is able to manage all the accounts without the necessity of appearing physically at a BIBD branch, thereby enjoying convenience and accessibility.

18. PW1 acknowledged that she is a registered user of the said App. She confirmed that she registered the said App through her VIVO 2130 mobile phone, linked to the number

+6738759939. The Bank acknowledged that the said registration process also allowed the BIBD system to record both her mobile number and the device brand and the device model number.

19. PW1 admitted that, to activate her use of the App, she had to "Agree" with the Terms and Conditions (T&C) of the said App. However, she admitted that she did not read the content of the T&C prior to clicking the "Agree" button. Despite this, PW1 admitted that she has consistently used the said App through the same mobile device and number for all doing her transactions. She confirmed that all six of her accounts are linked to her VIVO 2130 phone under the registered number, thereby consolidating her banking activities within the App.

Registration

20. PW1 agrees that she had registered her mobile number +6738759939 to register the said App. She agrees that phone brand is VIVO phone V1230. She acknowledged that her phone has a unique identification device 'da3d04111ecb563a' which will identify her as the user of the said App for each transaction made by her. The said reference was brought to PW1's attention and PW1 agrees that this page is a document generated by the BIBD System and she agrees with said content.

Method of Transfer:

21. PW1 provided detailed evidence regarding the process of conducting financial transactions through the BIBD Mobile Application in 2023.

22. She explained that access to her accounts required multiple layers of authentication. First, she had to enter her user ID and internet pin number. This was followed by selecting the mobile login option, which required the input of a mobile password. Thereafter, the system directed her to a further page where she was required to enter a double password consisting of eight characters. Only upon completing these steps was she able to gain access to all her accounts.

23. Once access was granted, a menu appeared enabling PW1 to select the type of transaction she intended to perform. If she wished to make a transfer or payment, she would press the relevant service button, which would then direct her to the appropriate page. In particular, PW1 explained that if she intended to transfer funds to a third party within BIBD, she would select the option "Transfer with BIBD (3rd Party)." The system would then display a list of recipients previously added to her "Favourite" list. She emphasized that transfers could only be made to individuals whose names were already included in this list.

24. PW1 further described the procedure for adding a new recipient to her "Favourite" list. This required pressing the "Add Favourite" button, entering the recipient's nickname and account number, and proceeding to the next page where the transferor's name appeared. The App would then prompt her to verify the details, after which a One-Time Password (OTP) would be delivered to her mobile phone. Upon entering the OTP into the App and confirming, the new recipient would be successfully added to her list of Favourites.

25. For the actual transfer, PW1 explained that she had to specify the amount and the account from which the funds were to be drawn. She would then confirm the transaction, which triggered another OTP request. The OTP was sent to her mobile phone, and upon entering and confirming it, the system displayed that the transfer was successful. PW1 stressed that this was the manner in which she personally authorised transactions in 2023.

26. PW1 clarified that her intention in presenting this evidence was to demonstrate the security measures and authorisation steps required in the mobile application, thereby showing the manner in which, she responsibly managed her transactions.

27. She further explained that the features she used in 2023 differs and had since been upgraded due to her financial loss by using the BIBD mobile app.

28. PW1 avers that the system in 2023 does not have the sufficient safeguards to protect customers' savings, and that BIBD was aware of these deficiencies, leading them to subsequently upgrade the application.

Advisories:

29. During cross-examination, PW1 initially denied receiving any messages or advisories from her Relationship Manager (RM). However, when confronted with documentary evidence contained at pages 68 and 69 of the Agreed Bundle of Documents (ABOD), she conceded that she had indeed received one advisory. PW1 agrees that this advisory is an invitation to the BIBD Hari Raya open house and a cautionary notice against online scams.PW1 was asked to read the Advisory.

30. PW1 agrees that the advisory specifically warned recipients to remain vigilant against individuals falsely claiming to represent BIBD, whose objective was to obtain sensitive personal information such as One-Time Passwords (OTPs) and debit card details. It further emphasised that BIBD would never request personal or banking information through phone calls or social media platforms. Practical guidance was also provided on how customers could safeguard themselves against such fraudulent attempts.

31. PW1 admitted that she had received the advisory but acknowledged that she did not read it.

Terms and Conditions:

32. PW1 admitted that she did not read the T&C governing the use of the said App. PW1 agrees that she had consented to the T&C when she registered the said App and that she is bound by the T&C when she activates the said App b.

33. PW1 agrees that she activated the said APP without reading the T&C and without understanding the obligations imposed upon her, including the indemnity clause (Clause 11) designed to protect the bank against customer non-compliance.

The Scam Call:

34. PW1 stated that she was not an IT expert and do not understand how the scam occurred. PW1 explained the two incidents in February and April 2023 where she merely answered an automated phone calls from individuals who claimed to be from BIBD. One of the automated calls were relating to a transaction approval and the other concerning internet banking access. She told the court that on both occasions she did not had a chance to respond as the call got cut off. PW1 told the court that she became suspicious that she alerted her RM, Md Khairuddin because the instructions given during the two calls differed. Her RM recommended her to cancel the debit card, which resulted in a replacement issued a week later.

35. On the 18th May 2023 PW1 received an automated phone call for the third time purportedly from BIBD regarding a transaction of B$3,000 that she did not transact. PW1 was at RIPAS Hospital because she was attending a medical appointment for headaches and blurred vision when she received the third call. She explained that the automated third call gave her the options to approve or to select customer service. She explained that she selected the option for customer service rather than approving the transaction, and maintained that she remained mentally alert throughout the incident.

36. The automated system connected her to a man who introduced himself as Jonathan, claiming to represent BIBD. Jonathan enquired about a B$3,000 transaction which PW1 denied making. Jonathan informed her that he would have to refer the matter to the BIBD Headquarters (HQ) and that another officer from the BIBD HQ would be contacted her.

37. Subsequently, PW1 received a call from a woman identifying herself as Michelle Ong from BIBD HQ. Michelle Ong stated that she had been informed by Jonathan of the disputed transaction and that she needed to investigate the matter. As part of the investigation Michelle Ong informed PW1 that she needs PW1's IC number, card number, full name, and date of birth in order to verify the transaction within the BIBD system.

38. PW1 was then told of an alleged outstanding credit card debt of B$7,700, which shocked her. Michelle Ong told her that she would have to investigate the matter further and instructed PW1 not to contact the bank directly but to communicate only via Telegram.

39. Shortly thereafter, PW1 received another call from a man identifying himself as Jeffrey, claiming to be from the BDCB Investigation Unit. Jeffrey explained that a report had been made through Michelle Ong and BCBD would have to investigate further. He requested for PW1's card and user ID details. PW1 did not suspect any fraud, except that the manner of his speech and the Malaysian accent he used seemed unusual. Jeffrey further informed her that Michelle Ong would contact her via Telegram and advised her not to make any transactions for five days.

40. On 23 May 2023, PW1 discovered that she could no longer access into her internet banking on her mobile phone. Using PW2's device, she found that unauthorized withdrawals totaling B$100,000 had been made, leaving her accounts with a balance of only B$106.

41. PW1 and PW2 immediately reported the matter to her RM (PW2) at BIBD Perdana branch. Her RM directed her to Ak Amalludin (DW1) the Perdana Branch Manager in Kuilap. She was then advised to make a police report. PW1 was subsequently informed that the funds had been transferred to a third-party account based on their internal investigation.

Self-Disclosure:

42. Based on the BIBD internal investigation, she was informed that the disputed transactions could only have been executed if she had shared the six-digit One-Time Password (OTP) with the third party.

43. PW1 recalled that an OTP had been sent to her VIVO device at 4.56 p.m., but she denied ever disclosing it. When confronted with the BIBD system (Page 33 of ABOD) record showing that the OTP had been validated through a Realme device, PW1 stated that she was unaware of this fact.

44. PW1 told the court that she did not realise that the personal information she had provided to Michelle Ong could reset her login credentials. She rejected the suggestion that her lack of awareness was unreasonable, maintaining that she did not understand the technical implications of the information she had shared. PW1 vehemently denied knowingly and assisting the third party in carrying out the fraudulent transactions.

Police Report:

45. The Plaintiffs alleged that their financial loss was attributable to the negligence of BIBD, contending that the bank's security system was flawed and that it owed a duty of care to

its customers. On this basis, they argued that BIBD should be held liable to compensate them for the loss sustained.

46. PW1 was confronted with the police report filed jointly with PW2. It was brought to her attention that the subject matter of the report is *Misuse of Computer Act*. In that report, both PW1 and PW2 stated that their account had been "digodam" (hacked). PW1 admitted that she was present during the filing but did not ask the officer what the term meant. Immediately thereafter, she provided her own police statement, which also employed the word "digodam,". PW1 denied misrepresenting facts to the police or failing to disclose her communications with Jonathan, Michelle, and Jeffrey during the first report.

47. PW1 was subsequently recalled by the CID Unit to provide another statement, during which she was cautioned about the criminal offence of giving false evidence. She admitted that it was only at this stage that she disclosed the incidents in February, April, and the events of 18 May 2023, her communications with Jonathan, Michelle, and Jeffrey

48. PW1 explained that she only realised she had been scammed when giving this later statement, acknowledging that it provided her with a clearer understanding of how the fraud had occurred.

Statement to Prosecution:

49. PW1 confirmed that she had given another statements to the Prosecution against the three defendants. These defendants were identified as the recipients of her money, accounts used by them to park the stolen funds.

50. PW1 was asked as to why she had not sued these three individuals directly, arguing that they were the ones who received her money. PW1 replied that she did not understand the law, that the defendants had not yet been convicted, and that she believed BIBD was negligent and owed her a duty of care. Defence Counsel suggested she could have redirected her claim against the recipients regardless of conviction, since they had received her money. PW1 agreed in principle but maintained her position that BIBD was responsible. Even when pressed to reconsider her affidavit considering her admissions, PW1 stood firm, insisting she would maintain her statement.

51. During re-examination, PW1 clarified that there were three scam incidents in total, though only two resulted in financial losses. The second incident involved the cancellation and re-issuance of her BIBD card. She confirmed that she had disclosed her card details, expiry date, CVV, and user ID to the scammers but denied providing any OTPs.

52. She further testified that she later discovered that the fraudulent transactions were executed from a Realme device. PW1 demonstrated to the Court the safeguards in the

present BIBD Mobile App. Noting that the current system had improved and was more secure than the 2023 version.

53. PW1 stated that she became aware of the full extent of the unauthorized transfers on 23rd May 2023, when she accessed the couple's joint accounts through her husband's mobile application. She discovered a total of 32 withdrawals, of which 6 were reversed, while 26 remained credited to third-party accounts. She emphasized that neither she nor the other plaintiffs received any email or SMS notification from the bank regarding these transactions.

54. PW1 admitted that she only read the advisory note issued by BIBD on 23rd May 2023. She confirmed that she had loss a total of $160,000. She maintained that BIBD had been negligent and owed her a duty of care to protect her monies from unauthorized access.

55. PW1 also testified that the bank had advised her to seek assistance from the police and the Brunei Darussalam Central Bank (BDCB). At that stage, she did not know the identities of the recipients of the monies and stated that had she known, she might have attempted to recover the money directly.

56. PW1 reiterated her belief that the bank had failed in its duty to protect the plaintiffs' monies and was therefore liable for the loss. She added that she could not recall where her initial statement was taken, admitted that she had mistakenly provided the wrong date of birth when signing it, and explained that she was in shock at that time. She also could not recall whether she received a copy of the statement from BIBD, but remembered that she and PW2 submitted their first police report, made at Berakas Police Station, to the BIBD Branch Manager as required by the bank.

57. In her re-examination, PW1 maintained that the bank advised her to seek help from the police and BDCB, reiterated that BIBD failed to protect her funds, and acknowledged errors in her initial statement, including a mistaken date of birth given while in shock, noting that she and PW2 submitted their first police report to the BIBD Branch Manager as required.

PW2- HAJI MAZLAN BIN HAJI ABD SAMAD

58. PW2, Haji Mazlan bin Haji Abd Samad, is the husband of PW1 and the primary account holder for both disputed BIBD accounts. He testified that he had entrusted PW1 to manage his bank accounts, including all online transactions through the BIBD Mobile App. PW2 stated that only he and PW1 knew the log-in credentials and internet banking PIN. He further submits that he personally never performed any transactions using the application, as all such activities were carried out by PW1 on his behalf. PW2 expressed his view that BIBD refused to accept responsibility for the loss of funds from his account.

59. During cross-examination, PW2 stated that he permitted PW1 to handle all mobile banking activities and that any transaction made by PW1 was done with his authority. He testified that he would not have approved the sharing of confidential banking information with third parties.

60. He then explained that the first time that he heard of these names, “Jonathan”, “Michelle Ong” and “Jeffrey” when he and PW1 went to BIBD Kiulap branch to inquire about the missing funds. He confirmed that it was during this visit that PW1 discovered the loss. He was uncertain whether he had heard those names prior to the visit. He recalled that PW1 made the report to the relationship manager at BIBD and informed them that she had not received any notification of the transfer. PW1 further emphasized that he cannot remember that the 3 persons scammed PW1.

61. PW2 stated that during the visit to BIBD Kiulap, PW1 did most of the talking. He then said that when he was at the police station, he filed the First Information Report (FIR), confirming that its contents were accurate. PW2 agreed that he filed the initial report under the “Misuse of Computer Act,” using the word *“digodam”* (hacked). He clarified that his understanding of the word “*digodam*”. He told that he had explained to the police that their account has been accessed without their permission and approval not hacked by other people. He equated “*hacking*” to unauthorized access, based on his understanding.

62. PW2 admitted that he did not know what personal information PW1 might have shared with the three individuals.

63. Three individuals and that he was unfamiliar with the terms and conditions of the BIBD Mobile App. He also said that he doesn’t know the terms and conditions of the Mobile App. He agreed to sue BIBD after he had the discussion with PW1 and he confirmed that he wasn’t sure if PW1 was the one who breached the mobile banking usage with BIBD that caused her to lose all the money.

64. During the re-examination, PW2 emphasised that he merely complied with his wife’s instruction to join BIBD Perdana and had no knowledge of any alleged breach by PW1. He further stated that he was unaware of the contents of the contract as he had not read it.

Court’s Finding:

65. Plaintiff sue BIBD for negligence and breach of duty of care for failing to provide as secure banking system. To prove negligence, the Plaintiff has to show:

    i. A duty of care owed to the Plaintiff

    ii. Defendant breach by failing to meet the standard of reasonable care

iii. The breach is the cause of the Plaintiffs financial loss and

iv. The Loss suffered by the Plaintiffs are not too remote.

66. I have given full consideration and proper weight to all the evidence presented before the Court. In doing so, I have taken into account the inconsistencies and contradictions that emerged in the testimony of each witness.

67. Having carefully assessed the evidence, the Court finds that the Plaintiffs' financial losses is not attributed to the Bank's negligence. I am satisfied that the losses arose from the conduct of PW1 herself. I am further satisfied that there was no fault in the banking system as it operated in 2023.

68. My reasoning is as follows:

Evidence of PW1 on Duty of care and breach:

69. I am satisfied that the Bank has exercise their duty of care when they issue the Advisory (Page 68 & 69 ABOD). The said advisory contained clear advisories warning customers never to share such information. PW1 acknowledged that she had received but failed to read these advisories and had not familiarized herself with the bank's terms and conditions, which expressly placed responsibility on customers to safeguard their credentials.

70. By PW1's testimony the Bank has demonstrated has exercise protective measures communicated to protect its customer. The Bank cannot be faulted for PW1 failure to take cognisance of the advisory's content.

Causation:

71. The cause of the unauthorised transaction is PW1 disclosing her Banking Credentials to the third party during the cross examination. She admitted to disclosing confidential information of her card details to individuals she believed were bank officers. I accept that PW1 may have subjectively believed the calls were genuine, but such belief does not excuse the absence of due diligence.

72. A reasonable person exercising ordinary caution would have questioned the requests for sensitive information, particularly considering widespread public awareness of telephone scams. Hence, the voluntary disclosures directly enabled the unauthorised transactions, establishing a causal link between her actions and the loss.

73. In the course of cross-examination, PW1 further accepts that once her personal and banking details had been disclosed, the third party were able to reset the mobile banking application without requiring any further involvement from her. She acknowledged that this disclosure gave the third party an independent control, enabling them to add beneficiaries and conduct transactions without her participation.

74. By virtue of PW1's admission, it confirms that the critical step which facilitated the unauthorised activity was caused by her own act of providing confidential information. By agreeing to this proposition, PW1 effectively conceded that the unauthorised transaction was made possible through her disclosure, rather than through any failure or compromise of the Bank's system.

75. PW1 in her cross examination admitted that, PW1 already knew she had been tricked by the third party. Even with this awareness, PW1 agrees that she chose not to disclose it. Instead, she tried and still shift the blame onto the Bank, suggesting that its system had been hacked.

76. PW1 also admitted that she told PW2 about her suspicion before they went to the branch. Despite this, both Plaintiffs stayed silent when making their complaint. This shows that they knew the real cause of the problem was the scam, but they deliberately hid this fact.

77. The Plaintiffs' reliance on subsequent improvements to the bank's mobile application is irrelevant, as the adequacy of security must be assessed against the standards prevailing at the time of the incident. Accordingly, I am of the view that the Plaintiffs' claim fails. The responsibility for the financial loss rests with the Plaintiffs themselves, and not with the bank.

78. I rejected PC submission that PW1's evidence was consistent and remain unrebutted under cross examination on the issue of disclosing her OTP, PIN, or credentials to the third party.

Remote:

79. As mentioned above, PW1 may have subjectively believed the calls were genuine, but such belief does not excuse the absence of due diligence.

Defendant's witnesses:

80. The totality of Defendants witnesses' evidence (DW1, DW2, DW3, and DW4) and the documents, in particular, the documentary evidence produced at page 39 ABOD presented before me, negate any suggestion of negligence. I am satisfied that the Plaintiffs' losses were not attributable to any fault in the bank's system and that its banking system was not compromised in 2023.

81. I now set out my reasoning. As stated above, I have considered what is pertinent, including the evidence elicited during cross-examination and re-examination. Having weighed the totality of the testimony and documents before me, I am satisfied that the Plaintiffs' losses were not attributable to any fault in the bank's system.

82. My reasoning are as follows:

DW1: Ak Amalluddin bin Pg Hj Muhammad

83. DW1 gave clear and consistent evidence and aligned with the documentary record shown at Page 39 ABOD, prepared by DW3. Both DW1 and DW3 corroborated each other in material respects.

84. I am satisfied that DW1 displayed a sound knowledge of his job scope and responsibilities, and he maintained his evidence without deviation under cross-examination or re-examination.

85. DW1 has provided independent evidence of his version of events that transpired on PW1's log-in transfer (Page 33 ABOD). This reflects both his expertise and familiarity with the technical aspects of the banking system. In addition to that the consistency between DW1 and DW3 strengthens the reliability of their evidence and demonstrates that the bank's records were accurately presented. On this basis, I find DW1 to be a credible witness whose evidence can be relied upon in determining the issues before the Court.

86. DW1 clarified that his role as branch manager did not include monitoring fraud or unusual transactions unless they were reported directly by customers, and that responsibility for safeguarding personal details rests with the customer.

Terms and Conditions (T&C):

87. DW1 explained that the duty of care to safeguard the customers Banking Credential lies with the customers only.

88. DW1's explained that this duty of care is stipulated in the T&C if the BIBD Mobil Banking App, which PW1 has contractually agree to abide.

89. I have read the relevant section of the T&C, the clauses are clear and unambiguous. These clauses impose clear obligations on the user which are directly relevant to this dispute and which the PW1 had agreed.

90. Under the T&C provision, PW1:

    i. undertook to provide the bank with true, accurate, and complete information, and to promptly notify BIBD of any changes.

    ii. It also provides that the Bank excludes any liability for any consequences arising from her failure to comply with these obligations.

iii. PW1 further undertook to maintain strict confidentiality over her User ID, PIN, OTP, passwords, and other security credentials. Where changes were necessary, she was permitted to reset such credentials only through the Mobile App or by contacting BIBD's service Centre.

iv. The bank disclaims liability for losses arising from unauthorized use of these credentials unless such losses are directly attributable to its gross negligence or willful misconduct.

v. PW1 also bore responsibility for notifying BIBD of any changes to her mobile number, with the bank expressly excluding liability for losses resulting from her failure to update such information.

vi. Importantly, the terms confirm that BIBD is not obliged to verify the validity of transactions once the correct credentials are entered, and it will not be liable if PW1's mobile device is used for unauthorized or fraudulent activity.

vii. In addition, PW1 expressly agreed to indemnify BIBD against claims, demands, or expenses arising from her use or misuse of the Mobile App, save where losses are directly caused by the bank's gross negligence or misconduct. Finally, as a joint account holder of all accounts except Account 4, PW1 owes duties to the other Plaintiffs to use the Mobile App responsibly and not in a manner that infringes their rights. These provisions collectively demonstrate that PW1 bore primary responsibility for safeguarding her credentials and ensuring proper use of the Mobile App, and that liability rests with her unless gross negligence by the bank can be shown.

91. Based on the BIBD systems, it shows that the third party had accessed to PW1's six joint account and explained that it is only possible if PW1 had disclosed sensitive information such as debit card numbers and PINs to the third party and that without such disclosure the unauthorized transfers could not have occurred.

The Breached:

92. DW1 finding is documented at page 39 of the ABOD. DW1 first explained the accounts handled by PW1. DW1 referred to paragraph 3 of his affidavit, D1. It shows the list of accounts held by PW1.

Plaintiffs' Account Details

Reference	Account No. / Initial as at 18.05.23	Account holder (s)	Account Type Single / Joint

"Account 1"	00-001-02-1160720 $404.38	1.1st Plaintiff 2. 2nd Plaintiff	- Wakalah - Joint
"Account 2"	00-001-02-0038917 $100,106.13	1. 1st Plaintiff 2.2nd Plaintiff	- SA Saving - Joint
"Account 3"	00-001-02-0748157 $6,166.87	1. 1st Plaintiff 2. 4th Plaintiff	- Wakalah - Joint
"Account 4"	00-020-02-0018361 $48,331,85	1. 1st Plaintiff	- SA Saving - Single
"Account 5"	00-010-02-0124726 $4,741.69	1. 1st Plaintiff 2. 3rd Plaintiff	- SA Saving - Joint
"Account 6"	00-001-02-1365484 $3,642.34	1. 1st Plaintiff 2.5th Plaintiff	- Wakalah - Joint

93. Following PW1's Police report, DW1 informed the court that BIBD conducted an internal investigation on the unauthorised transactions. As a result of the said internal investigation, PW1's log-in Attempt was generated. This generated document was produced and exhibited at page 39 of ABOD. It is labeled as 1st Plaintiff's Login Attempt-FATIMAHJAYA. This document shows the following log-in attempt made on PW1's account.

Log-in Attempts- FATIMAHJAYA

No	Date	Time	Device ID	Phone make	Phone model	Successful login	Remarks	Push Notification sent Device
1	17/5/2023	11:54:13	da3d04111ecb563a	vivo	V2130	Yes		
2	17/5/2023	13:55:07	da3d04111ecb563a	vivo	V2130	Yes		
3	17/5/2023	14:10:51	da3d04111ecb563a	vivo	V2130	Yes		
4	18/5/2023	15:04:30	da3d04111ecb563a	vivo	V2130	Yes		
5	18/5/2023	16:58:57	82afcaf7ba777c84	realme	RMX33581	yes	Internet PIN reset was performed at 16:56:42 successfully and OPT sent	Sent @ 16:58:58

							at 16:56:43 to phone number +6738759939 (OTP validated successfully with OPT code 462808). Mobile password was entered successfully with no reset perform	
6	18/5/2023	17:05:45	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @ 17:05:45
7	19/5/2023	0:40:36	Cb7e51ec2312f2df	Xiaomi	22120RN86G	Yes		Sent @0:40:36
8	19/5/2023	0:45:07	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @0:45:08
9	19/5/2023	9:25:08	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @9:25:08
10	19/5/2023	9:43:13	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @9:43:13
11	19/5/2023	10:00:39	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @10:00:39
12	19/5/2023	10:20:13	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @10:20:14
13	19/5/2023	21:20:53	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @21:20:54
14	20/5/2023	8:58:41	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @8:58:42
15	20/5/2023	10:08:02	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @ 10:08:02
16	20/5/2023	10:14:44	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @ 10:14:44
17	20/5/2023	22:58:25	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @ 22:58:26
18	21/5/2023	20:14:21	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @ 20:14:25
19	21/5/2023	20:14:59	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @ 20:15:00
20	22/5/2023	9:55:05	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @ 9:55:06

21	22/5/2023	12:39:37	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @ 12:39:38
22	22/5/2023	12:42:44	82afcaf7ba777c84	Realme	RMX3581	Yes		Sent @ 12:42:45

94. DW1 explained that:

i. Item 1-4, dated- 17- 18/5/2023 @ 15:04:30- PW1's account was logged in using the Vivo phone.

ii. Item 5 dated - 18/5/2023 @ 16:58;57- Internet PIN reset was performed at 16:56:42 successfully and OPT sent at 16:56:43 to phone number +6738759939 (OTP validated successfully with OPT code 462808). Mobile password was entered successfully with no reset perform successfully a sent to a device ID 82afcaf7ba777c84 on a Realme, RMX3581.

iii. Item 6-22- 18-22/5/23- Login in was made successfully to the Realme phone.

iv. DW1 explained that this document shows that there was a total of 26 transactions were carried out across six accounts, amounting to B$160,000 between 18 and 22 May 2023. DW1 provide a chart to show the said transfer (Table B of Paragraph 16, D1 and Paragraph I Tabe C of the DEFENCE):

95. DW1 explained that from this log-in:

i. Account 1 shows that there was a single transfer of $300 to Account 4.

ACCOUNT 1			
No.	**Date**	**To Bank Account**	**Transfer Amount (BND)**
1	22.05.2023	Account 4	$300.00

ii. Account 2 recorded the largest activity, with multiple transfers ranging from $7,500 to $9,500 directed to third-party accounts, totaling over $90,000.

ACCOUNT 2			
No.	**Date**	**To Bank Account**	**Transfer Amount (BND)**
2	18.05.2023	18010004842 (3rd Party)	$8,000.00
3			$9,000.00

4			$7,500.00
5 6			$8,500.00 $9,000.00
7			$8,000,00
8	19.05.2023	8010010613 (3rd Party)	$9,000.00
9			$8,500.00
10			$9,500.00
11			$8,000.00
12			$7,500.00
13			$7,500.00

iii. Account 3 reflected a $6,000 transfer to a third party and a small internal transfer of $66 to Account 4.

ACCOUNT 3			
No.	**Date**	**To Bank Account**	**Transfer Amount (BND)**
14	20.05.2023	8010010613 (3rd Party)	$6,000.00
15	22.05.2023	Account 4	$66.00

iv. Account 4 itself registered several transfers, including $8,000, $9,500, $5,000, $6,000, and a final $10,000 to third-party accounts.

ACCOUNT 4			
No.	**Date**	**To Bank Account**	**Transfer Amount (BND)**
16	20.05.2023	8010010613 (3rd Party)	$8,000.00
17			$9,500.00

18			$9,500.00
19			$5,000.00
20			$6,000.00
21			$6,000.00
22	22.05.2023	10010002849 (3rd Party)	$10,000.00

v. Account 5 contained two internal transfers of $4,500 and $141 to Account 4,

ACCOUNT 5			
No.	**Date**	**To Bank Account**	**Transfer Amount (BND)**
23	22.05.2023	Account 4	$4,500.00
24			$141.00

vi. Account 6 showed similar internal movements of $3,500 and $42. In total, $160,000 was transferred to third parties, with $8,549 moved internally between the plaintiffs' accounts.

ACCOUNT 6			
No.	**Date**	**To Bank Account**	**Transfer Amount (BND)**
25	22.05.2023	Account 4	$3,500.00
26			$42.00
		TOTAL TO 3RD PARTIES	**$160,000.00**
TOTAL TRANSFERRED WITHIN THE ACCOUNTS			$8,549.00

No Breach:

96. DW1 explained that Item 5, the remarks shows that the transactions were executed using valid login credentials, which the Bank considered to be legitimate and did not require further verification. Hence, the transaction did not flag as suspicious.

97. Based on DW1's explanation it is only reasonable to conclude that PW1 had inadvertently disclosed her confidential information and the OTP which had enabled the third parties to gain authenticated access to her mobile app.

98. I reject PC submission that the Defendant's attempt to shift blame, based on alleged disclosure of a card number and OTP, are speculative. I accept Defence argument that there is no plausible explanation as to how the OTP could have been used successfully without PW1's involvement, given that it was sent to her Vivo mobile phone.

99. I accept DW1's evidence that when this matter was reported to the Police, the bank froze the third-party accounts and referred the matter to the Financial Crime Compliance unit, to investigate. He maintained that the bank had no obligation to intervene earlier because the transactions were authenticated through proper login procedures.

100. For the said reason, I accept DW1's explanation that the loss was caused by the PW1's actions and for the said reason, the Plaintiffs' claim of negligence against BIBD could not be sustained.

DW2: Muhammad Khairuddin bin Haji Musa

101. DW2 served as the Relationship Manager (RM) for PW1 under BIBD's PERDANA Privilege Banking services. In this capacity, he was responsible for providing tailored financial advice, facilitating transactions, and maintaining a direct mobile communication channel to ensure efficient and prioritised assistance for all of her banking needs. His role extended beyond routine account management to include safeguarding the Plaintiff's awareness of security risks.

102. DW2 informed the court that he regularly shared BIBD's customer advisories on mobile security, online scams, and fraudulent transactions, supplementing the notices published on the Bank's platforms with personalised reminders sent directly to the 1st Plaintiff via WhatsApp.

103. On 5 May 2023, DW2 sent an "Important Information" advisory in Malay, warning against impersonation scams and emphasising that BIBD would never request personal or banking details through phone or social media. The advisory highlighted the need for vigilance, urging customers not to disclose confidential information, not to transfer funds to unknown parties, and to verify suspicious calls. This message was read by the PW1.

104. On the 23rd May 2023, when PW1 reported being unable to access her mobile banking app and discovered a drastic reduction in the balance of her joint account, DW2 immediately referred the matter to the Perdana Kiulap Branch Manager for further handling.

105. His actions demonstrate that his role was both advisory and responsive: ensuring the Plaintiff was informed of security risks, and promptly escalating issues when irregularities were detected hence complying their duty of care to all their customers.

106. PC submits that DW2, who had direct contact with the 1st Plaintiff after the incident, conceded that no alerts were generated and no steps were taken to notify or protect the account during the breach period. I accept his role as a Relationship Manager was primarily advisory and customer-facing, not investigative or technical. This issue is address by DW4.

DW3: Haji Abdul Hasif Bin Hj Osman:

107. DW3 is the BIBD Senior Retail Solution Officer attached with the Information Technology Division. His evidence centered on the records contained at Page 39 of the ABOD which records the login attempts and the transactions associated with PW1's Mobile Banking Application.

108. Referring to Page 39 of ABOD, he confirmed the first four items (Item 1-4) on the record were made from PW1's Vivo phone. However, beginning with Item 5 from the 18 May 2023, the transactions were conducted through a different device, identified as a Real Me phone. DW3 explained that this shift occurred because the internet PIN had been reset successfully, a process requiring validation through a One-Time Password (OTP) sent to the account holder's registered number. He emphasized that if a third party had knowledge of the user ID, mobile password, and internet PIN, they could gain full access to the account, even from a different device.

109. Turning to page 44 of the ABOD, DW3 addressed the transactions involving the PW2. He further confirmed that withdrawals of $7,500 (page 41) linked to the joint account were executed through PW1's app, not PW2's app, which explained why notifications were sent only to PW1's device. Page 43 of the ABOD showed that the transactions were carried out using the Real Me device, but DW3 maintained that because the credentials were entered successfully, the transactions were considered authorized by the bank.

110. DW3 conclude that the takeover of PW1's mobile app by the Real Me device was only possible because the necessary credentials (the user ID, mobile password, internet PIN, and OTP) had been disclosed or compromised. DW3 rejects the allegation that the Mobile App's security measures were at fault, attributing responsibility instead to PW1 disclosure of sensitive information.

111. I accept DW3's technical explanation of "authorisation". I accept DW3's evidence that transactions are deemed authorised once the correct credentials—namely the Username, Internet PIN, and Mobile Password—are successfully entered. DW3 repeatedly emphasised that the Bank's system recognises such use of credentials as valid authorisation, regardless of whether the account holder personally initiated the transaction. This position was consistently maintained throughout his evidence and was corroborated by the documentary records. I, therefore, rejected PC submission that DW3's effort to distinguish between "device registration" and "OTP validation" was unconvincing and appeared to be semantic deflection rather than a meaningful explanation of security architecture. DW3 explanation was clear.

112. I rejected the contention that authorisation required the express agreement of the account holder for each transaction. As DW3 had demonstrated that the Bank's system operates on credential-based validation, and once those credentials are correctly provided, the transaction is treated as authorised. I find DW3 explanation logical, consistent and supported by the records before it.

113. I take note that under the 2023 system, such access was treated as authorized if credentials were correctly entered, regardless of the device used. However, he noted that subsequent system changes now prevent access from non-registered devices, thereby addressing the vulnerabilities highlighted in PW1 and PW2's case.

114. Accordingly, I accept DW3's finding of fact and rejects the allegation advanced by Plaintiff's Counsel. I find there is no breach.

DW4- Abdul Fitri Shah @ Abdul Fattah Haji Mohd Ali

115. DW4 is the Information Security Manager at BIBD. He was asked to investigate whether the bank experienced any cyberattacks between 18 May and 22 May 2023. This request came after a customer claimed that 26 unauthorized transactions, totaling B$160,000, had occurred during that time.

116. DW4 provided a clear and comprehensive account of the Bank's security framework and its operation during the relevant period. DW4 confirmed that while the Bank relied on static OTP protocols without device binding, and conceded that no alerts were triggered for new device logins or large-value transactions, these features did not amount to systemic failure.

117. He explained that the SIEM platform was not designed to generate such alerts if the transactions are validated by correct credentials. It will be treated as legitimate. Importantly, DW4 confirmed that internal audit raised no concerns, and that subsequent security upgrades were introduced only after the Plaintiffs' loss.

118. I accept DW4's explanation to be consistent with the documentary record. His evidence demonstrated that BIBD maintained a multi-layered defense system, including the Information Security Department, Cyber and IT Risk Management, and Internal Audit, all of which operated effectively at the time. He further confirmed that the Security Operations Centre detected no cyber incidents between the 18th and the 22nd May 2023, and that independent compromise assessments conducted in July 2023 found no evidence of hacking or unauthorised access.

119. Based on DW4's explanation, I reject the allegation advanced by Plaintiff's Counsel that the Bank's security was inadequate or that the system had been breached. DW4's evidence establishes that the unauthorised transactions were not the result of any cyberattack or systemic failure, but arose because the necessary credentials had been disclosed. On this basis, I accept DW4's testimony and dismisses the Plaintiffs' claim of hacking.

Negligence and Breach:

120. The Plaintiff is claiming against the Defendant for negligence and breach of duty of care arising from unauthorised transfer totaling $160,000 form their respective accounts.

121. Based on the finding above, my findings are as follows.

Duty of Care:

122. I am satisfied that the T&C of the Banking Mobile App is clear on the obligation of the Bank. I am satisfied that Clauses 3.1.4 and 8.6 shift the responsibility to the customers to safe guard their personal banking credential and that the Bank bears no responsibility for losses arising from unauthorised access where the Plaintiffs' own credentials were used, even if those credentials were disclosed to third parties. Clause 8.4 further establishes that the Bank is under no obligation to investigate or verify the validity of a transaction once the correct credentials have been entered, as such transactions are deemed authorised by the system. Finally, Clause 10 confirms that the Bank owes no duty to provide features or safeguards beyond those available in the Mobile App at the time the transactions were effected.

123. Taken together, these provisions make clear that the Defendant's duty is limited to operating the Mobile App as designed, and liability does not extend to losses caused by the Plaintiffs' disclosure of credentials or expectations of features not provided under the contract.

Breach of Duty:

124. I dismiss the Plaintiffs argument that the Bank had breached its duty of care by failing to detect and block suspicious activity, pointing to the unusual pattern of high-frequency, high-value transfers as red flags which should have triggered the Bank.

125. I accept DW4 explanation that that the SIEM platform was not designed to generate such alerts if the transactions are validated by correct credentials and that it will be treated as legitimate.

126. I dismiss the said allegation for the reason mentioned above (Duty of Care) as the Plaintiffs are bound by clause 8.4 of the Mobile App agreement. Clause 8.4 makes clear that once the correct credentials are entered and a transaction is successfully executed, the Bank has no duty to investigate or verify its validity. Its obligation is to process instructions, not to second-guess them.

127. The evidence from DW1 and DW3 confirms that the unauthorised transfers were all carried out using PW1's valid and authenticated credentials. The system data showing login activity (page 33 of ABOD) was accepted by PW1, and it is undisputed that her User ID, amended Internet PIN, Mobile Password, and OTP were correctly entered. The successful reset of the Internet PIN granted full access to her mobile app, including joint accounts, enabling the transactions to proceed.

128. I am also satisfied the Bank had discharged their duty by sending clear advisories warning customers not to disclose confidential information, which PW1 admitted receiving it but chose to ignore. DW4 further confirmed that no cyberattack or breach was detected during the relevant period, and that independent assessments found no evidence of hacking. On this evidence, the Court is satisfied that the Defendant did not breach its duty of care.

129. On these facts, I find that the transactions were properly authorised under the system. The Defendant was under no contractual duty to monitor or detect patterns of use, but rather bound to execute valid instructions promptly.

130. I rejected PC allegations that BIBD's security framework in May 2023 as fundamentally defective. The evidence of the Defence witness should not be read in isolation. I am satisfied that the overall evidence given by the Defence witness show no systemic failures nor a breach of duty in contract or tort.

131. I accept DW4 evidence that the absence of real-time fraud alerts or device-specific triggers cannot be equated with negligence. Fraud detection systems are designed with thresholds and parameters that balance efficiency, customer convenience, and operational realities. The fact that alerts were tied to account balances above BND 100,000 reflects a rational prioritization of resources, not a systemic collapse.

132. On the issue of OTP, I am satisfied that at the material time, BIBD's authentication measures were consistent with prevailing standards in the region. The subsequent enhancements introduced after May 2023 were proactive improvements, not admissions of prior inadequacy. Continuous upgrading of systems is a hallmark of responsible banking, not evidence of liability.

133. The suggestion that relationship managers should have detected anomalies misconstrues their role. RMs are tasked with client servicing, not real-time fraud surveillance. I accept that expecting them to monitor every transactional behaviour across multiple accounts is unrealistic and beyond the scope of their professional function.

134. I accept all banks regularly update systems to meet new threats. I accept PW3 and DW4s' explanation that progress does not mean past failure. I accept that the Bank's systems were working within accepted norms, and there is no basis to say they failed or breached any duty.

Causation:

135. I find that the losses suffered by the Plaintiffs were caused by PW1's own actions in voluntarily disclosing confidential banking information to third parties. PC repeatedly submits that PW1 did not disclosed her Personal Banking Information to the third party. But PW1 had admitted under cross-examination that she did disclose her card details and OTP to individuals she believed were bank officers, and later realised she had been scammed. She further conceded that she and PW2 remained silent about this realisation when making their complaint. DW3's evidence established that the takeover of PW1's mobile app was only possible because these credentials had been compromised by PW1's voluntarily disclosure. The proximate cause of the loss was therefore the Plaintiffs' own disclosure of sensitive information, not any failure by the Bank.

136. I, therefore, dismiss and reject PW1 allegation that she did not disclosed her banking personal information to the third party.

Remoteness:

137. In this case, the losses flowed directly from the Plaintiffs' voluntary disclosure of credentials. They were not a foreseeable consequence of any act or omission by the Defendant, but rather of the Plaintiffs' own conduct. Accordingly, the requirement of remoteness is not satisfied.

Failing to Redirect:

138. I reject PC submission on the Defence failure for electing not to re-examine it witnesses, suggesting that such failure lead to an adverse inference and to accept the cross-examination evidence as credible and uncontradicted. And failure to re-examine

has treated as further confirmation of Defendant's liability in both negligence and breach of contract.

139. The law on re-examination is well settled. Section 138(3) of the Evidence Act (CAP 108) provides that re-examination shall be directed to the explanation of matters referred to in cross-examination, and only with the court's permission may new matters be introduced. The purpose of re-examination is therefore limited: it exists to clarify or reconcile discrepancies between examination-in-chief and cross-examination. It is not a mechanism to reargue the case or to undo concessions properly elicited under cross-examination. The discretion lies entirely with counsel to determine whether clarification is necessary.

140. The Plaintiff's reliance on ***Brown v Dunn*** **(1893) 6 R 67 (HL)** is misplaced. That authority establishes the principle that a party must put its case to opposing witnesses during cross-examination, failing which adverse inferences may be drawn. It does not impose any obligation on a party to re-examine its own witnesses. The absence of re-examination cannot, in itself, justify an adverse inference.

141. Counsel must exercise judgment in deciding whether re-examination is necessary. Where no discrepancies arise, re-examination serves no purpose. The decision not to re-examine cannot be treated as a failure or omission, but rather as a proper exercise of discretion. The credibility of the witnesses and the weight of their testimony must be assessed on the totality of the evidence, not on whether re-examination was undertaken.

142. I agree that re-examination is a discretionary tool, not a mandatory obligation. It arises only where clarification is required to reconcile inconsistencies.

Conclusion

143. Applying the principles of negligence to the facts, I am satisfied that the Plaintiff owe a duty to protect and safe guard her Personal Banking Credential. The Plaintiffs' case fails because the evidence shows that the transactions were enabled by their own disclosure of confidential information. I do not find the Defendant to be liable for the Plaintiffs' financial loss. Responsibility for the financial loss rests with the Plaintiffs, not the Defendant.

144. For the said reason, I dismiss the Plaintiffs' claim in its entirety with costs to the Defendant.

Indemnity:

145. The Defendant seek costs and legal award on a solicitor-client full indemnity basis.

146. I refer to Clause 11.1 of the Mobile App Terms and Conditions. By agreeing to using the Mobile Banking facilities, the Plaintiffs expressly agreed to indemnify the Defendant against any claims, demands, expenses, or liabilities, including full legal costs, arising from their use of the Mobile App. This indemnity applies to situations where losses result from the Plaintiffs' own actions, such as misuse of the App or its content, breach of the contractual terms, or infringement of third-party rights connected to their access or use.

147. I further note that PW1 openly admitted she had no genuine intention to sue the Defendant. Her claim was pursued only because, at the time of filing, she did not know the identities of the third parties who had misappropriated the funds. PW1 acknowledged that once those identities became known, she could and should have directed her claim against them rather than the Defendant. She further conceded that continuing this suit was unnecessary and that it ought to have been withdrawn.

148. PW1's evidence demonstrates that the Plaintiffs commenced proceedings against the Defendant not because of any culpability on its part, but out of desperation when the true wrongdoers were unknown. By July 2024, the Plaintiffs had identified the recipients of the funds yet persisted with their claim against the Bank.

149. I accept the Defence submission that such conduct, tantamount to an abuse of process. I further accept that the Plaintiffs cannot rely on ignorance of the law, having been represented by counsel throughout.

150. Accordingly, I find the Plaintiffs' losses were caused by PW1's own conduct, and that maintaining this claim against the Defendant when the proper parties were long identified reveals the absence of any sustainable cause of action. The Defendant has been subjected to unnecessary litigation, and costs are warranted.

151. I therefore allow the Defendant to claim cost and legal fees on a solicitor-client on full indemnity basis.

PG MASNI PG HJ BAHAR
Judge, Intermediate Court