

**IN THE UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

HARBORVIEW CAPITAL PARTNERS,
LLC,

Plaintiff,

vs.

CROSS RIVER BANK,

Defendant.

Docket No. 2:21-cv-15146-EP-SDA

**PLAINTIFF HARBORVIEW CAPITAL PARTNERS' SECOND
AMENDED COMPLAINT**

CHIESA SHAHINIAN & GIANTOMASI PC

A. Ross Pearlson, Esq.
Brigitte M. Gladis, Esq.
105 Eisenhower Parkway
Roseland, NJ 07068
Telephone: 973.325.1500
Facsimile: 973.325.1501

**FRANKEL, RUBIN, KLEIN, PAYNE
& PUDLOWSKI, P.C.**

Mayer S. Klein, Esq. (admitted *pro hac vice*)
231 S. Bemiston Avenue, Suite 1111
Clayton, MO 63105
Telephone: 314.725.8000
Facsimile: 314.726.5837

*Attorneys for Plaintiff
Harborview Capital Partners, LLC*

Plaintiff, Harborview Capital Partners, LLC (“Plaintiff” or “Harborview”), by and through its undersigned counsel, for its Second Amended Complaint against Defendant Cross River Bank (“Defendant”, “Cross River” or “Bank”), alleges as follows:

PARTIES

1. Plaintiff Harborview is a Delaware limited liability company authorized and existing under the laws of Delaware.

2. Defendant Cross River is a New Jersey banking corporation with its principal place of business in Teaneck, New Jersey.

JURISDICTION AND VENUE

3. Plaintiff is a Delaware limited liability company, and Defendant is a New Jersey entity. For this reason, there is diversity of citizenship between the parties.

4. The amount in controversy exceeds \$75,000.

5. Venue is proper in this Court since Defendant is a resident of the State of New Jersey, and Plaintiff’s cause of action arose in New Jersey.

FACTS

6. Cross River was established in 2008, with Mr. Gilles Gade (Gade) as President. Cross River’s primary place of business is 885 Teaneck Road, Teaneck, New Jersey 07666.

7. Mr. Ephraim Kutner (Kutner) is President of Harborview.

8. Gade and Kutner had a longstanding social relationship. They were friends for many years, and had worked together on various charities.

9. Kutner formed Harborview with his brother, Jonathan Kutner (collectively “the Kutners”). Harborview is a commercial real estate finance, equity, and advisory firm which provides services for all commercial real estate asset classes.

10. Harborview's business includes high-dollar transactions. The business is located in the United States, and its work is limited to the United States. Harborview has never conducted any business outside the United States.

11. In 2013, Gade and Kutner discussed Harborview, specifically whether Harborview would set up accounts for its significant business in Cross River Bank.

12. At all relevant times herein, Gade was keenly knowledgeable as to Harborview's business, basically what the business was about and how it operated, that the business operated only in the United States, that Kutner traveled extensively in furtherance of the business, and the particular needs for security that a business like Harborview required.

13. In various communications, Gade communicated both with Kutner and internally with Cross River personnel about Harborview setting up its accounts at Cross River, and was involved in getting the accounts established at the Bank.

14. Upon information and belief, Gade knew that securing Harborview's business would significantly improve Cross River's financial status by growing its modest base of assets/deposits, and would effectively advance the Bank's reputation as a reputable financial institution. The addition of Harborview's business would benefit Cross River in multiple ways.

15. In response to Cross River's efforts to secure Harborview's business and the deposit of its significant funds, Harborview expressed and communicated its primary concern with depositing such significant assets in a financial institution like Cross River. Harborview clearly communicated its concerns and questions as to whether the Bank had the resources and ability to handle and securely protect Harborview's funds. For Harborview, that concern also included questions as to whether the Bank had the personnel, policies, and procedures which would protect

Harborview's assets and which were readily available in other and larger financial institutions where Harborview could take its money.

16. In order to convince Harborview to set up its accounts at Cross River, Gade assured and promised Kutner personally on behalf of Cross River and on multiple occasions that Harborview's money would be safe. Gade also discussed several other ways that he, Cross River, and Harborview could work together.

17. Gade also assured and promised Kutner that Cross River's top people would always be readily accessible to handle Harborview's needs.

18. Harborview relied on Gade's promises and representations, made on behalf of Cross River, that Cross River would keep Harborview's money safe.

19. Cross River expected and intended that Harborview would rely on these promises and representations, and Harborview reasonably relied on same.

20. At all relevant times herein, communications between Harborview and Cross River were conducted primarily, particularly on any issues of concern, between Gade and Kutner or other top management personnel in the two organizations.

21. Gade would routinely communicate with Kutner to inquire as to whether Harborview was satisfied with the Bank's services, whether Harborview was happy with the Bank's services, and whether Harborview had any other needs.

22. Harborview understood Gade's inquiries and discussions as indicating that Gade was directly involved with ensuring that Harborview's accounts were being protected as promised.

23. Based on Gade's representations, Kutner understood and believed that Cross River would be utilizing all means necessary to protect Harborview's money, and that the Harborview accounts would be watched over by Gade or other top management personnel of the Bank.

24. Harborview would not have deposited funds in Cross River if not for the representations and promises made by Gade on behalf of Cross River.

25. In reliance on Kutner's relationship and discussions with Gade, on Gade's knowledge of Harborview's business, and on Gade's representations that Cross River would take the steps necessary to protect Harborview's assets, Harborview began depositing funds at Cross River. Such deposits ultimately totaled the sum of \$20,000,000.00, within various accounts at Cross River.

26. Upon information and belief, Gade was personally involved in and supervised the set up of the Harborview accounts.

27. For example, Gade negotiated the details of the interest rate which would be applied to certain accounts.

28. In addition, Gade personally offered Harborview additional incentives such as offering not to *ever* charge Harborview for being overdrawn on a savings account if the company kept certain balances in other accounts.

Opening Accounts

29. In order to initiate the opening of accounts for Harborview, Cross River required that Harborview complete certain forms.

30. Upon information and belief, Tina Rubino, a branch manager for Cross River, was the person assigned to handle the mechanics of setting up the accounts.

31. Upon information and belief, Gade was supervising and in contact with Ms. Rubino during this process.

32. Ms. Rubino consulted Gade directly with Harborview questions, and responded to Harborview with Gade's directions regarding how the accounts would be set up.

33. In or about January 2018, Ms. Rubino provided Harborview with a business account data form.

34. On information and belief, completion of the business account data form utilized by Cross River is required by and is in accordance with the applicable banking regulations and commensurate with the industry standard for obtaining the information required to protect each customer's funds.

35. Ms. Rubino indicated that the business account data form would have to be filled out in order to open the account and prepare signature cards.

36. Upon information and belief and based on her email communications, Ms. Rubino carefully scrutinized the completed account data form, and identified what additional information was required to connect the account to online banking. This is standard procedure under the bank's Know Your Customer Policy, as it using these forms to give every client a "risk rating" based on the business conducted of the customer.

37. In January 2018, Harborview, as it had done many times prior, completed and returned the business account data form required by Cross River. *See Exhibit A: Account Opening Data Entry Form/New Business Account Information* (account data form).

38. The account data form provided the following required information:

- a. Anticipated Wire Activity: **Domestic** 6
 Foreign 0
- b. Monthly \$ Volume **Domestic:** \$6,8000,000.00
Monthly \$ Volume **Foreign:** 0
- b. Trade Area: **USA**
- c. Is Business Conducted of Foreign Nature: **No**

39. On the same account data form, Harborview designated the following Authorized

signers:

- a. Ephraim Kutner
Position with the Company: President and CEO
Owner of Account: Yes
- b. Jonathan Kutner
Position with the Company: Managing Director and Principal
Owner of Account: No
- c. Marilyn Tirado/Bara Dolinger/Gershon Yarmush
Position with the Company: **Administrative Staff**
Owner of Account: No

40. In addition to the communications between Kutner and Gade and the communications with Ms. Rubino, Harborview completed all account data forms with the same information; i.e. Harborview's Trade Area was "USA"; its Anticipated Wire Activity was "Domestic"; and the business it conducted was *not* of a foreign nature. *See e.g.*, **Exhibit B**. Ms. Rubino denoted the risk rating as "High" based on her review of the anticipated activity.

41. Harborview consistently and repeatedly advised Cross River that it did not conduct foreign business and did not make foreign wire transfers. In addition, as the result of a "high" risk rating, Cross River's Know Your Customer (KYC) policy required Cross River to "identify and understand the general operating" environment and the "relationship with a particular customer within their target market." See KYC Policy, **Exhibit C, p.13**.

42. Cross River's owner, Gade, who promised Kutner that Cross River would keep Harborview's money safe, knew that Harborview did not conduct foreign business and did not make foreign wire transfers.

43. Harborview employed all means known to it to convey to and ensure that Cross River knew that Harborview did not make foreign wire transfers, none of its Authorized Signers

was permitted to authorize foreign wire transfers, and Cross River had or would put in place the necessary procedures to ensure that foreign wire transfers were not processed from any Harborview account. Harborview's Authorized Signers were given no authority to change the business practices of Harborview as told to Cross River.

44. Upon information and belief, if Harborview had indicated that it would be conducting foreign wire transfers, additional information and steps would have been required to allow Harborview to process foreign wire transfers. Since Harborview clearly indicated that it would *not* be employing foreign wire transfers, Cross River did not provide any information or otherwise discuss foreign wire transfers with Harborview.

45. Harborview understood that one of the purposes of the account data form was to provide the information Cross River required to protect the funds in Harborview's accounts.

46. Harborview understood that the account data form was the method set up by Cross River for Harborview to communicate to the Bank how its account was to be handled, and it was Harborview's expectation that Cross River would allow only domestic wire transfers as Harborview clearly instructed on the account data form.

47. Upon information and belief, one of the purposes, if not the primary purpose, of requiring that the customer identify whether it conducts domestic and/or foreign wire activity and whether it conducts foreign business is to identify what type of transfers the named signatories were designated to authorize.

48. Upon information and belief, if Cross River had no policies and procedures in place by which it would scrutinize wire transfers, but Cross River would instead allow any signatory to authorize any type of transfer without reference to the customer's directions, then there would be no need to require that the customer identify the types of transfers its signatories were allowed to

authorize.

49. Upon information and belief, the information elicited on the account data form was input in Cross River's system and utilized in order for Cross River to institute or apply policies and procedures which would ensure that wire authorizations were limited to either Domestic or Foreign as indicated by the customer, and so that Cross River could take the steps necessary to (1) limit the persons who could authorize a transfer to only those individuals identified on the account data form, and (2) limit transfers to the type of transfer identified on the account data form.

50. Harborview reasonably relied on Cross River to review and utilize the instructions and information provided in the account data forms in order to protect Harborview's monies as promised.

51. Cross River expected and intended that Harborview would rely on Cross River's proper use of the information provided on the account data entry forms to enact or apply policies and procedures to protect Harborview's monies, and Harborview reasonably relied on same.

52. Cross River failed either to correctly document the information Harborview provided on the account data form, and/or Cross River negligently failed to institute and/or apply procedures which would have prevented the processing of a foreign wire transfer in direct contravention of the information Harborview provided at Cross River's direction.

53. The documents completed as required by Cross River indicate that the Authorized Signers were authorized for domestic wire transfers only.

FRAUDULENT TRANSFERS

54. At some point prior to August 16, 2018, unbeknownst to Harborview, the CEO of Harborview's e-mail account was hacked.

55. The hacker added a rule to auto-delete all mail to the CEO's email inbox, which

allowed the hacker to send and receive emails from the CEO's account without the CEO's knowledge.

56. From August 16, 2018 through August 27, 2018, the hacker used the CEO's email account to direct an administrative staff person to wire funds internationally.

57. This hacking scheme was well known in the banking industry as "CEO Fraud" or "Business Email Compromise."¹

58. By 2018 when the fraudulent Wire Transfers were processed by Cross River, this type of wire fraud was well-known in financial circles as the "Business Executive Scam" or the "CEO Fraud."² The FBI described the scam as follows:

The e-mail accounts of high-level business executives (CFO, CTO, etc) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing these requests.

59. As early as 2015, the FBI reported that "the majority of the [fraudulent] transfers" in CEO Fraud and other Business Email Compromise cases, were "going to Asian banks located within China and Hong Kong."³

60. On July 12, 2018, the FBI reported that the real estate industry was a particular target of Business Email Compromise schemes.⁴

61. Despite the industry knowledge of the way CEO Fraud schemes work, and the particular vulnerability of companies in the real estate sector, Cross River failed to set up

¹ See further information *infra* at 57 et. seq.

² See, Federal Bureau of Investigations Internet Crime Complaint Center. (2016). Business email compromise: The 3.1 billion dollar scam. Retrieved from: <http://www.ic3.gov/media/2016/160614.aspx>. See also, Ensign, Rachel Louise. (23 Feb 2020). Losing \$450,000 in Three Days: Hackers Trick Victims into Big Wire Transfers; Wall Street Journal (Online); New York, N.Y.

³ See, Federal Bureau of Investigations Internet Crime Complaint Center. (2015). *Business email compromise public service announcement*. Retrieved from: <https://www.ic3.gov/media/2015/150827-1.aspx>.

⁴ See, Federal Bureau of Investigations Internet Crime Complaint Center. (2018). *Business E-Mail Compromise The 12 Billion Dollar Scam*. Retrieved from <https://www.ic3.gov/media/2018/180712.aspx>.

appropriate heightened security procedures to catch potential CEO Fraud/Business Email Compromise, particularly in light of Cross River's knowledge that Harborview did not conduct foreign wire transfers.

62. As a result of the hacking scheme, Cross River processed four (4) international wire transfers ("Wire Transfers") from Harborview's Account as follows: \$420,000.00 on August 16, 2018; \$95,000.00 on August 17, 2018; \$325,000.00 on August 24, 2018; and \$955,000.00 on August 27, 2018.

63. Each transfer was directed to Hang Seng Bank in Hong Kong, an entity that was flagged by Cross River's Office of Foreign Asset Control control software on each of the Wire Transfers.

64. Upon receipt of each foreign wire transfer form, Cross River verbally contacted only Harborview's administrative staff person despite the fact that Cross River knew that the individual was allowed to authorize only domestic wire transfers to verify the authenticity of the wire.

65. Cross River conducted the authorization process with the administrative staff person in the exact same manner as it conducted authorizations for domestic wire transfers. Despite the information Harborview made available to Cross River and Cross River's knowledge of its customer, or its duty to know its customer, Cross River did not question or discuss with the administrative staff person the particulars of this transfer.

66. Cross River's acts and omissions were negligent and in direct contravention of the policies and procedures which should have triggered a commercially reasonable procedure to confirm whether the foreign wire transfer was authorized.

67. Cross River's failure to determine if these were authorized transfers was also

contrary to its practice of monitoring Harborview's accounts and questioning any transactions it considered suspicious.

68. In or about February 2018, Cross River questioned a deposit into a Harborview account and demanded that Harborview provide documentation supporting the deposit of that particular sum of money.

69. Unlike its handling of the February 2018 deposit into a Harborview account, Cross River did not conduct any investigation or require any documentation to support the withdrawal of money from a Harborview account by foreign wire transfer, as it was required to per its own KYC policy

70. Based on Cross River's efforts and procedures for monitoring funds deposited into Harborview's accounts, Harborview reasonably believed and expected that Cross River was exerting the same effort and applying the relevant procedures for monitoring the disbursement of Harborview funds.

71. The administrative staff person that Cross River contacted regarding a wire transfer to Hong Kong was a signatory for authorizing domestic wire transfers only. As a result of its negligence in failing to obtain an authorization for a foreign wire transfer, Cross River is liable for processing an unauthorized wire transfer to Hong Kong.

72. Based on the information Cross River solicited from Harborview as well as Gade's and Cross River's ongoing communications with the Kutners and Harborview, Cross River knew or should have known that a transfer of funds to a foreign entity was not authorized, and could not be authorized by administrative staff.

73. For these reasons, Cross River knew or should have known that the lack of an authorization for a foreign wire transfer required that Cross River utilize commercially reasonable

procedures to determine whether the transfer of funds to a foreign entity, particularly a transfer to Hong Kong, a well-known location for fraudulent transfers, was indeed authorized by the owner of the account.

74. Harborview reasonably relied on its communications with Cross River and Gade's assurances and promise that Harborview's money would be protected to expect that policies and procedures were in place or would be enacted to protect Harborview's funds including, but not limited to, the policies and procedures required to ensure that the Bank would not allow for an unauthorized foreign wire transfer.

75. For these same reasons, Harborview reasonably expected that Cross River had in place commercially reasonable security measures which met the minimum industry standard procedures for protecting Harborview's accounts including, but not limited to, coding Harborview's accounts so as to allow for the processing of only domestic wire transfers and the flagging of foreign wire transfers particularly for transfers to well-known centers for fraudulent activity such as Hong Kong.

76. Upon information and belief, Cross River had or should have had policies and procedures in place to ensure—since Harborview had not identified a signatory for a foreign wire transfer—that any attempts to conduct a foreign wire transfer would be barred pending the application of commercially reasonable procedures to ensure the proper authorization for a foreign wire transfer.

CROSS RIVER'S RELIANCE ON PURPORTED AUTHORIZATION.

77. Cross River was not entitled to rely on the purported authorization it obtained from an administrative staff person who was authorized only for domestic wire transfers for the following reasons:

a. Cross River had or should have had internal policies and procedures, in addition to industry-standard procedures, for heightened security in place and which it should have applied for scrutinizing a foreign wire transfer, particularly where it knew the customer did not conduct foreign wire transfers, and where the transfer was directed to Hong Kong to an entity which Cross River knew or should have known Harborview had never done business with;

b. Cross River conducted the authorization process for a foreign wire transfer form for a transfer to Hong Kong in the exact same manner as it did all domestic wire transfers despite its knowledge that (1) the administrative staff person was not designated to authorize foreign wire transfers, and (2) the form designated a transfer to Hong Kong, a location which the Bank, not its customer, knew was a prime destination for fraudulent transfers. After obtaining the required signatures, Cross River called only the administrative staff person, as it would a domestic wire transfer, to confirm authorization—the exact same process used for domestic wire transfers with no enhanced procedures for a foreign wire transfer.

c. Cross River knew that Harborview did not conduct foreign wire transfers. Despite this knowledge, Cross River sent a foreign wire transfer form to a person not designated to authorize a foreign wire transfer, and conducted the same process for authorization as it utilized for a domestic wire transfer. Unlike it had done in challenging a deposit to a Harborview account where it discovered potentially suspicious activity, Cross River did not conduct any additional questioning, require additional documentation, or in any other manner investigate the proposed foreign wire transfer as required under its own internal procedures and/or universally-accepted procedures requiring a higher degree of scrutiny for a foreign transfer particularly to a location such as Hong Kong;

d. Specifically, Cross River did not conduct a “heightened due diligence” review of four

wires being sent to Tier 3 county as required by both its KYC and OFAC policies. This is despite the OFAC software flagging each of the wires as a “potential match” before Cross River’s staff deeming it a “false positive” for every one of the wires;

e. Cross River failed to inform the customer that the recipient bank was flagged as a “false positive” or that the wire room manager who made the determination that it was a false positive did not regularly have her determinations audited, did not have regular training, or did not have her practices aligned with bank practices;

f. Cross River knew that Harborview did not conduct foreign business and did not make foreign wire transfers. The account opening form information was available to all Cross River employees, including the wire room staff at all times in Cross River’s customer information database;

g. Despite this change in Harborview’s business practice, Cross River did not conduct an investigation in Harborview, a “high risk” client. As required by its own KYC policy, when a “triggering event”, including “changes in the nature of the account activity” occur, Cross River’s policy requires a “site visit[] of high risk customers.” **Ex C, p. 12.** No such site visit occurred;

h. Cross River’s policy requires it to monitor for “significant changes in activity, ownership, or public information about the client become known.” To accomplish this, Cross River states that “The Bank uses an automated monitoring system in order to monitor account activity, on an ongoing basis” and that this would be monitored on “a daily basis.” **Ex. C, p. 20-21.** This daily review should have caught unusual activity related to “OFAC Screening”, “return item[s]” and when “wire transfers that have no apparent business purpose to of from a foreign country” that are “inconsistent with the customer’s legitimated business purpose.” **Ex. C, p. 21-22.** As a result of these daily reviews, Cross River mandated it would be “initialing the Daily Account

Review Log or the report printout.” **Id.** This was not done and as such Cross River was not monitoring its customer’s authorizations as its own policies require;

i. Cross River’s policy identifies that as to certain customers, there could be a higher vulnerability to “identify theft, embezzlement, and fraudulent schemes.” As a result, the KYC policy is designed to protect and look out for such patterns. While this policy is geared towards “elderly individuals”, Cross River clearly had the means to identify fraudulent schemes but did not employ it to a “high risk” account;

j. Cross River knew of the existence of CEO fraud and how it operated and Harborview’s particular susceptibility to said type of fraud. Based on its uniquely particular knowledge of Harborview’s business, Cross River was in the position, and had assured Harborview it was in the position, of taking the steps necessary to protect Harborview’s funds;

k. Cross River knew that the signatories on the account data form were designated only for domestic wire transfers, and were not designated to authorize foreign wire transfers;

l. In order to secure Harborview’s business for Cross River’s benefit, Gade personally assured Harborview that Cross River would keep Harborview’s money safe thereby implicitly guaranteeing that Cross River had or would institute and apply the policies and procedures required to protect Harborview’s funds;

m. Based on Gade’s personal representations and promises and Cross River’s practice of monitoring Harborview’s accounts and contacting Harborview about any activity Cross River deemed suspicious, Cross River led Harborview to reasonably rely on and expect that Cross River was monitoring Harborview’s account transfers, and would personally notify either Kutner or other top management personnel of Harborview of any activity that was not in accordance with Harborview’s written directions for account activity; namely, that only domestic wire transfers

being could be authorized without additional scrutiny and investigation;

n. Cross River's practices due either to ignorance of its Harborview customer—or in deliberately choosing to ignore the knowledge of its customer—were in contravention of standard industry practices and its own policies and procedures, especially in light of Cross River's unique knowledge of and familiarity with Harborview's business; and

o. Cross River's OFAC policy failed to provided sufficient protections from money ending up in the hands of foreign bad actors.

CROSS RIVER'S RESPONSE TO THE FRAUDULENT TRANSFERS

A. Cross River failed to promptly advise Harborview of the failed foreign wire transfer.

78. The initial foreign wire transfer of August 16, 2018 failed to properly process from Cross River to Hang Seng Bank. Such failure occurred on August 16, 2018, and continued on August 17, 18, 19, 20, and 21, 2018 with such foreign wire transfer failing to successfully occur each time.

79. Each of the Fraudulent Transfers was subject to an OFAC "potential match". Cross River's wire room manager flagged all wires as "false positives". Cross River failed to identify why so many consecutive, suspicious wires were all flagged as "false positives". Had Cross River engaged any security procedure, due diligence, or heightened due diligence into "false positives", such as comparing the hits against the business practices of Harborview, it would have immediately identified that the fraudulent transfers were "suspicious activity" as identified by its own policies and procedures.

a. Cross River's OFAC policy also failed to "address how it will determine whether an initial OFAC hit is a valid match or false hit" as stated in the "Bsa/aml Manual"

released by the FFIEC.⁵

b. Cross River employees failed to provide a sufficient memo or log of why the False Positive determination was made.

c. Cross River's "daily" audit failed to identify these false positives or flagged so many false positives consecutively from the same entity.

80. On August 17, 2018, Cross River learned that the initial foreign wire transfer of August 16, 2018 was not successful. Yet, in contravention of industry standard security policies and procedures for Harborview's protection, Cross River failed to notify Harborview about the failed foreign wire transfer until August 21, 2018.

81. Specifically, on August 21, 2018, five (5) days after Cross River processed the initial foreign wire transfer, Cross River first notified Harborview that the August 16, 2018 wire transfer did not successfully transfer in contravention of the industry-standard security policies and procedures which were or should have been in place and applied for Harborview's protection.

82. By failing to advise Harborview that the August 16 wire transfer did not successfully transfer from August 16, 2018 through August 21, 2018, Cross River allowed the matter to remain unresolved for five days. While the initial foreign wire transfer of August 16, 2018 was not successful, the remaining three (3) foreign wire transfers, totaling the sum of \$1,375,000.00 were successfully completed.

83. None of the foreign wire transfers would have been made but for Cross River's failure to (1) obtain proper authorization for a foreign wire transfer, and/or (2) follow commercially

5

<https://bsaaml.ffiec.gov/manual/OfficeOfForeignAssetsControl/01#:~:text=The%20bank's%20policies%2C%20procedures%2C%20and,match%20or%20a%20false%20hit.&text=Due%20diligence%20steps%20for%20determining,on%20the%20OFAC%20Web%20site.>

reasonable procedures to timely notify Harborview of the failed initial unauthorized foreign wire transfer.

84. Upon information and belief, Cross River either failed to institute or failed to follow industry standard policies and/or the applicable federal banking regulations when it failed to obtain the required authorization for a foreign wire transfer and further failed to timely notify Harborview as to the failed wire transfer. This allegation is pled upon information and belief as Cross River has failed and refused to turn over to Harborview the applicable banking policies that Cross River maintained at the time of the subject failed wire transfer.

B. Cross River failed to investigate the failed foreign wire transfer.

85. In addition to failing to obtain the required authorization and failing to timely notify Harborview of the failed August 16, 2018 foreign wire transfer, Defendant also failed and refused to investigate the cause of the failed foreign wire transfer in accordance with the minimum industry standards for said investigation.

86. Cross River failed to exercise due diligence in order to determine the cause of the failed wire transfer in accordance with commercially reasonable procedures and minimum industry standards.

87. Contrary to Gade's prior history of direct communication with the Kutners regarding important issues, neither Gade nor any of the "readily accessible" top management personnel personally and directly contacted Kutner. Instead, Cross River informed only sent an email on August 21, 2018, indicating that the wire did not successfully transfer.

88. Cross River did not try to identify the source of the failure, nor did it reasonably investigate why Cross River's numerous attempts at resending the August 16, 2018 foreign wire transfer failed.

89. This lapse in security on Cross River's part exemplifies Cross River's negligent failure to institute and/or follow the minimum industry standards for providing the protection Gade and Cross River had promised Kutner and Harborview.

90. Had Cross River properly and reasonably investigated the failure of the August 16, 2018 foreign wire transfer in accordance with the promised security policies and procedures and minimum industry standards, Cross River would have discovered that it had not obtained the required authorization for a foreign wire transfer and thereby prevented the ensuing unauthorized transfers.

91. The loss of \$1,375,000.00 by Harborview would not have occurred but for Cross River's failure to obtain the required authorization or to have implemented the commercially reasonable security procedures for avoiding an unauthorized transfer and which required that Cross River investigate the cause of the failed August 16, 2018 foreign wire transfer.

92. The foreign wire transfers set forth above were not authorized by Harborview. The loss of \$1,375,000.00 by Harborview would not have occurred but for Cross River's negligence in processing an unauthorized foreign wire transfer.

93. Despite the facts that (1) Harborview had made 1,171 solely domestic wire transfers, (2) Gade and Cross River had indicated that policies and procedures were in place or would be put in place to insure the security of Harborview's funds, (3) Cross River had elicited and was responsible for knowledge of the information that Harborview's accounts would be used for domestic wires only, and (4) Cross River knew or should have known that administrative staff persons were authorized only for domestic wire transfers, Cross River allowed for an unauthorized foreign wire transfer of Harborview funds.

94. At no point did Cross River utilize commercially reasonable procedures to confirm authorization including, but not limited to, obtaining direct verbal authority from the President or Managing Director of Harborview for the process of a foreign wire transfer.

95. Given that the foreign wire transfers were international wire transfers as opposed to domestic wire transfers, and that Cross River knew or should have known Harborview's prior instructions and directions, as well as Harborview's established banking patterns, Cross River was required to utilize commercially reasonable procedures including, but not limited to, contacting the President and CEO and/or the Managing Director of Harborview to verbally confirm the authenticity of these Wire Transfers.

96. Further, given that (1) CEO Fraud was well known in the banking industry, (2) all of Harborview's prior wires were done domestically, (3) Cross River knew that the foreign wire transfers in question were going to Hang Seng Bank located in Hong Kong, Cross River should have utilized commercially reasonable procedures including, but not limited to, contacting the President and CEO and/or the Managing Director of Harborview directly to verbally confirm the authenticity of these wire transfers.

97. Cross River exhibited bad faith in failing to directly contact the President and CEO and/or the Managing Director of Harborview or take other commercially reasonable procedures to confirm the authenticity of the foreign wire transfers.

98. Cross River negligently failed to utilize additional commercially reasonable procedures including, but not limited to, obtaining two distinct contacts within Harborview to verify the authenticity of the foreign wire transfers.

99. The loss of \$1,375,000.00 by Harborview would not have occurred but for Cross River allowing an unauthorized transfer and failing to utilize commercially reasonable procedures

including, but not limited to failing to verbally contact the President and CEO and/or the Managing Director of Harborview regarding the Wire Transfers.

C. Cross River failed to follow commercially reasonable banking practices and its own security measures to prevent CEO Fraud.

100. Since Cross River processed the unauthorized and fraudulent foreign wire transfers, \$1,375,000.00 in funds belonging to Harborview were transferred to unauthorized third parties.

101. Cross River had an obligation to know its customer and was aware or should have been aware that Harborview did not conduct business with any foreign entity including, but not limited to, the account holders at Hang Seng Bank in Hong Kong.

102. Despite the industry knowledge of the way CEO Fraud schemes work, and the particular vulnerability of companies in the real estate sector, Cross River failed to set up appropriate heightened security procedures to catch potential CEO Fraud/Business Email Compromise, particularly in light of Cross River's knowledge that Harborview did not conduct foreign wire transfers.

103. As a result, in an act of bad faith and in breach of commercially reasonable security procedures, Cross River negligently processed the foreign wire transfers though they reeked of known fraud: (1) they were unauthorized transfers; (2) the CEO of Harborview was known to travel frequently, as is typical in CEO Fraud cases; (3) the wires were directed to a bank in Hong Kong, one of two countries known since at least 2015 to receive the large majority of fraudulent CEO Fraud wires; and (4) Harborview, a real estate company particularly vulnerable to CEO Fraud, had never previously wired ANY funds internationally.

104. Cross River displayed bad faith and commercially unreasonable security procedures when it failed to safeguard against the well-known CEO Fraud when setting up its security and confirmation procedures; industry knowledge of how CEO Fraud works should have

informed the development of commercially reasonable security procedures.

105. The actions of Cross River, as set forth above, violated acceptable and reasonable banking practices and procedures. As such, Cross River's actions were not taken in good faith and were not commercially reasonable.

106. Further, upon information and belief, Cross River failed to follow its own security procedures.

107. As noted above, Cross River continues to refuse to provide Harborview with a copy of the security procedures in place at the time of the relevant wire transfers.

108. Cross River's refusal to provide Harborview with its security procedures is contrary to standard banking practice and, upon information and belief, a violation of Cross River's own practices and procedures.

109. Further, upon information and belief, Cross River's refusal to provide Harborview with Cross River's security procedures suggests that Cross River violated its own procedures, and that Cross River violated standard banking practice and commercially reasonable banking standards.

110. Lastly, upon information and belief, since the events described in this Complaint, Cross River enacted new and revised policies and/or procedures to prevent the recurrence of the errors it made in this case. Cross River's actions effectively acknowledge the inadequacy of its former procedures as well as the feasibility of simple precautionary measures that it failed to implement previously.

111. The loss of \$1,375,000.00 by Harborview would not have occurred but for Cross River's allowing an unauthorized foreign wire transfer, and Cross River's failure to establish and/or adhere to commercially reasonable security standards.

D. Cross River failed to recover the improperly wired funds.

112. The foreign wire transfer funds were received at Hang Seng Bank by various account holders.

113. Such account holders maintained their bank account at Hang Seng Bank, which is an affiliate bank of HSBC, and principal member of the HSBC Group.

114. After the funds were fraudulently wired to the account holders at the HSBC affiliate, Cross River continued to act negligently and in bad faith by failing to demand that the HSBC affiliate return to its customer (Harborview) the wire transfer funds that were improperly processed by Cross River.

115. Further, Cross River learned that the account holders in Hang Seng Bank – the recipients of the fraudulent wire transfers – maintained numerous accounts in Hang Seng Bank, an affiliate of HSBC. Yet, Cross River failed to take reasonable steps and measures to recover the funds from the HSBC affiliate.

116. Cross River failed to act in good faith in allowing an unauthorized foreign wire transfer and in failing to comply with commercially reasonable security procedures when processing the wire transfers and failed to take reasonable steps and measures to recover the Wire Transfers once they were improperly processed, which constitutes gross negligence and carelessness on behalf of Cross River.

117. In allowing an unauthorized foreign wire transfer, Cross River failed to institute and/or comply with universally-accepted business protocols, practices and procedures instituted and applied by all United States banks including, but not limited to, the know-your-customer requirements of the Patriot Act.

118. In allowing an unauthorized foreign wire transfer, Cross River failed to adhere to

the universally-established business protocols, practices and procedures instituted and applied by all United States Banks, including but not limited to those policies and procedures universally applied where the transfers or transactions involve high crime areas, such as Hong Kong, and including, but not limited to the know-your-customer requirements of the Patriot Act.

119. In allowing an unauthorized foreign wire transfer, Cross River acted negligently and negligently failed to institute, utilize, and apply internal business protocols, industry-standard policies and procedures which are universally accepted and applied by all United States Banks.

COUNT I

(Violation of N.J.S.A. 12A:4A-201, 12A:4A-202 and 12A:4A-203)

120. Plaintiff incorporates the allegations of paragraphs 1-119 as if more fully set forth herein.

121. N.J.S.A. §§ 12A:4A-201, -202 and -203 govern the issuance and acceptance of payment orders by a bank.

122. N.J.S.A. § 12A:4A-201 sets out the definition of a “security procedure.”

123. Pursuant to N.J.S.A. § 12A:4A-202(1), “A payment order received by the receiving bank is the authorized order of the person identified as sender if that person authorized the order or is otherwise bound by it under the law of agency.”

124. Pursuant to N.J.S.A. § 12A:4A-202(2):

If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) **the security procedure is a commercially reasonable method of providing security against unauthorized payment orders**, and (ii) the bank proves that it **accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer** restricting acceptance of payment orders issued in the name of the customer. [Emphasis added.]

125. Pursuant to N.J.S.A. § 12A:4A-203:

(1) If an accepted payment order is not, under section 12A:4A-202(1), an authorized order of a customer identified as sender, but is effective as an order of the customer pursuant to section 12A:4A-202(2), the following rules apply:

(a) By express written agreement, the receiving bank may limit the extent to which it is entitled to enforce or retain payment of the payment order.

(b) The receiving bank is not entitled to enforce or retain payment of the payment order if the customer proves that the order was not caused, directly or indirectly, by a person (1) entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure...

126. Pursuant to N.J.S.A. § 12A:4A-202(1) and § 12A:4A-203, Cross River had a duty to transfer Harborview funds solely subject to an authorized payment order.

127. Cross River did not receive an authorized payment order in that the person identified as the sender was not authorized to send a foreign wire transfer.

128. Pursuant to N.J.S.A. § 12A:4A-202(2), Cross River had a duty to establish commercially reasonable security procedures regarding wire transfers.

a. According to Cross River's Wire Room Policy, the use of a phone call is designed to authenticate and verify a wire. The Wire Room Policy does not denote that a phone call in any way is designed to be a security procedure or that the phone call should try to determine whether the wire was being fraudulently generated.

b. Cross River's reliance on a phone call does not appropriately fall under the determination of a security procedure as no questions were asked by Cross River's employees about the nature of the transaction or that the transaction was a deviation from the pattern or practice of a high-risk customer.

129. Cross River further had a duty to safeguard the monies of Harborview by transferring funds only through an accepted payment order under §12A:4A-202(1), or ensuring

that the order was an accepted payment order under 12A:4A-202(2), by establishing and following commercially reasonable security procedures.

130. Cross River further had a duty to safeguard against known hacking schemes affecting the banking industry through establishing and following commercially reasonable security procedures.

a. Cross River failed to establish procedures that were sufficiently monitored on a daily basis that were required by the policies themselves.

b. Cross River failed to provide sufficient training and alignment to its own staff as to all its employees to understand the difference between an authorization call and a security procedure.

c. Cross River failed to maintain a written policy to identify fraudulent schemes such as CEO Fraud.

d. Cross River failed to conduct an investigation into a high-risk client having a “triggering event”.

131. Cross River also had a duty to accept the payment order only if it was an authorized payment order or was effective pursuant to N.J.S.A. § 12A:4A-202(2).

132. Cross River had a duty to know its customer, including but not limited to the wire transfer instructions provided by Harborview when they initially opened their accounts, and the pattern of behavior that Harborview established following said openings.

133. As set forth in all preceding paragraphs herein, Cross River violated the provisions of N.J.S.A. § 12A:4A-202(2) by processing unauthorized Wire Transfer orders in connection with the Account.

134. As set forth in all preceding paragraphs herein, Cross River violated the provisions

of N.J.S.A. § 12A:4A-202(2) by failing to maintain and/or adhere to commercially reasonable security procedures to confirm whether the proposed foreign wire transfer was authorized.

135. As set forth in all preceding paragraphs herein, Cross River violated the provisions of N.J.S.A. § 12A:4A-202(2) by failing to maintain and/or adhere to a commercially reasonable security procedure, which failure led directly to the theft of \$1,375,000.00 from Harborview's Account by unauthorized transfers, of which Harborview informed Cross River immediately upon discovery of said unauthorized transfers.

136. In addition, as set forth in all preceding paragraphs herein, because Cross River, at a minimum, (i) failed to ensure that it was transferring funds subject to an authorized transfer order, (ii) failed to utilize commercially reasonable security procedures including, but not limited to verbally confirming authorization for the transfers with the President and CEO and/or the Managing Director of Harborview, or obtaining two verbal confirmations, (iii) failed to apply its extensive knowledge of Harborview's banking patterns and practices, (iv) failed to institute and/or follow the applicable security procedures and policies, (v) failed to account for known CEO Fraud schemes in its security procedures, and (vi) failed to maintain adherence to its own internal bank policies, including but not limited to its Wire Room Policy, its Know Your Customer Policy, and its OFAC policy.

137. Accordingly, pursuant to N.J.S.A. § 12A:4A-203, the wire transfers were unenforceable. Nevertheless, Cross River effectuated the transfers.

138. N.J.S.A. § 12A:4A-204 states that if:

(1) a receiving bank accepts a payment order issued in the name of its customer as sender which is (i) not authorized and not effective as the order of the customer under section 12A:4A-202, or (ii) not enforceable, in whole or in part, against the customer under section 12A:4A-203, the bank shall refund any payment of the payment order received from the customer to the extent the bank is not entitled to enforce payment and shall pay interest on the refundable amount calculated from the

date the bank received payment to the date of the refund.

139. Given the foregoing, pursuant to N.J.S.A. § 12A:4A-204, Cross River is liable for its payment of unenforceable transfers, and thus must refund to Harborview the \$1,375,000.00 stolen by way of the fraudulent transfers together with interest at the highest rate allowed by law from August 27, 2018, and court costs.

WHEREFORE, Plaintiff, Harborview Capital Partners, LLC prays for judgment against Defendant Cross River Bank on Count I of its Complaint in the principal sum of \$1,375,000.00, together with interest at the highest rate allowed by law from August 27, 2018, court costs, and for such other and further relief as this Court deems just and proper.

JURY DEMAND

Plaintiff demands trial by jury of all claims and defenses in this action so triable.

By: /s/ A. Ross Pearlson

CHIESA SHAHINIAN & GIANOMASI PC

A. Ross Pearlson, Esq.
Brigitte M. Gladis, Esq.
105 Eisenhower Parkway
Roseland, NJ 07068
Telephone: 973.325.1500
Facsimile: 973.325.1501

**FRANKEL, RUBIN, KLEIN, PAYNE
& PUDLOWSKI, P.C.**

Mayer S. Klein, Esq. (admitted *pro hac vice*)
231 S. Bemiston Avenue, Suite 1111
Clayton, MO 63105
Telephone: 314.725.8000
Facsimile: 314.726.5837

*Attorneys for Plaintiff
Harborview Capital Partners, LLC*

Dated: October 30, 2025