UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

BANGLADESH BANK, Plaintiff, - against - RIZAL COMMERCIAL BANKING CORPORATION, MAIA SANTOS DEGUITO, ANGELA RUTH TORRES, LORENZO V. TAN, RAUL VICTOR B. TAN, ISMAEL S. REYES, BRIGITTE R. CAPIÑA, NESTOR O. PINEDA, ROMUALDO S. AGARRADO, PHILREM SERVICE CORP., SALUD BAUTISTA, MICHAEL BAUTISTA, CENTURYTEX TRADING, WILLIAM SO GO, BLOOMBERRY RESORTS AND HOTELS, INC. D/B/A SOLAIRE RESORT & CASINO, EASTERN HAWAII LEISURE COMPANY, LTD. D/B/A MIDAS HOTEL & CASINO, KAM SIN WONG A/K/A KIM WONG, WEIKANG XU, DING ZHIZE, GAO SHUHUA, and JOHN DOES 1-25, Defendants.	:	No. _____ **COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Bangladesh Bank, the central bank of Bangladesh ("**Plaintiff**," "**Bangladesh Bank**," or the "**Bank**"), by and through its attorneys, Cozen O'Connor, as and for its Complaint against Defendants, Rizal Commercial Banking Corporation ("**RCBC**"), Maia Santos Deguito ("**Deguito**"), Angela Ruth Torres ("**Torres**"), Lorenzo V. Tan ("**Lorenzo Tan**"), Raul Victor B. Tan ("**Raul Tan**"), Ismael S. Reyes ("**Reyes**"), Brigitte R. Capiña ("**Capiña**"), Nestor O. Pineda ("**Pineda**"), Romualdo S. Agarrado ("**Agarrado**," collectively with RCBC, Deguito, Torres, Lorenzo Tan, Raul Tan, Reyes, Capiña, and Pineda, the "**RCBC Defendants**"), Philrem Service Corp. ("**Philrem**"), Salud Bautista ("**Salud Bautista**"), Michael Bautista ("**Michael Bautista**," and together with Salud Bautista, the "**Bautistas**"), Centurytex Trading ("**Centurytex**"), William

So Go ("**So Go**," collectively with the RCBC Defendants, Philrem, the Bautistas, and Centurytex, the "**Banking-Related Defendants**"), Bloomberry Resorts and Hotels, Inc. d/b/a Solaire Resort & Casino ("**Solaire Casino**"), Eastern Hawaii Leisure Company, Ltd. d/b/a Midas Hotel & Casino ("**Eastern Hawaii Leisure**"), Kam Sin Wong a/k/a Kim Wong ("**Wong**"), Weikang Xu ("**Xu**"), Ding Zhize ("**Ding**"), Gao Shuhua ("**Gao**," collectively with Solaire Casino, Eastern Hawaii Leisure, Wong, Xu, and Ding, the "**Casino-Related Defendants**"), and John Does 1-25 ("**Doe Defendants**") (all of the foregoing, collectively, the "**Defendants**"), alleges as follows:

SUMMARY OF ACTION

1. This litigation involves a massive, multi-year conspiracy to carry out one of the largest banks heists in modern history right here in New York City. On February 4, 2016, thieves reached into a bank account at the Federal Reserve Bank of New York ("**New York Fed**") and stole approximately $101 million (out of the nearly $1 billion they attempted to steal). The bank account was held for the benefit of Bangladesh Bank, which is Bangladesh's Central Bank. Bangladesh Bank has had a 45-year banking relationship under which it has placed its international reserves with the New York Fed. The New York Fed is a critical component of the United States' central banking system and its link to the international financial system.

2. The conspiracy was seamless, with every complicated step plotted out in advance. The conspirators included North Korean hackers who had already broken into the computer systems of Sony Pictures Entertainment ("**Sony**"). Just as they did with Sony and tried to do with other banks, the North Korean hackers broke into Bangladesh Bank's computer systems. Indeed, the hackers that broke into the Bank's systems and caused the fraudulent payment instructions to be delivered to the New York Fed used malicious computer malware to access necessary servers, retrieve files and data, create files, change file names, steal credentials and login information,

including to the SWIFT system, erase key files and histories, and digitally cover their tracks. They then sent fraudulent payment orders to the New York Fed, for the explicit purpose of stealing money from Bangladesh Bank's New York Fed account and sending it out of the United States.

3. To accomplish this, the North Korean hackers aligned with co-conspirators in the Philippines, most importantly, RCBC, a bank in the Philippines that also had (and, on information and belief, continues to have) correspondent bank accounts at intermediary banks in New York City. The conspirators used RCBC's New York City correspondent accounts to receive the fraudulent transfers from the New York Fed via the New York Fed's Fedwire system, which was developed and is maintained by the Federal Reserve System and almost instantaneously transfers large-dollar payments.

4. Use of the Fedwire system in New York was critical to the conspiracy, as it allowed the thieves to quickly transfer the funds to the intermediary banks. From there, the intermediary banks, through RCBC's correspondent accounts, quickly transferred the stolen funds out of New York City and the United States to fictitious U.S. dollar accounts in the Philippines, which RCBC created nearly a year earlier to receive the stolen funds from New York.

5. Once the stolen funds were in the Philippines, RCBC and other co-conspirators, including questionable businesses, casinos, and individuals, executed a series of intentionally complicated account transfers and foreign exchange transactions to launder the Bank's stolen funds, all of which were eventually withdrawn from RCBC and brought to casinos and gambling junkets in the Philippines into which they disappeared.

6. In all, these thieves walked away with $81,001,662.12 from Bangladesh Bank's account in New York City, as the thieves were unable to get their hands on $20 million of the $101

million in funds originally stolen because a Sri Lankan bank returned them due to irregularities, rather than launder them in the way that RCBC did.

7. This highly-complicated, intricately planned heist of tens of millions of dollars from New York City only worked because of the coordination of the conspiracy and enterprise established among the Defendants, each of whom, as set out in great detail below, played their parts well. Each of these Defendants profited from the theft, some quite handsomely.

8. This litigation is the culmination of several years of work by the Bank to recover the funds stolen from its account in New York at the New York Fed, which, along with hundreds of other central government banks and international depositors, remains the key location for Bangladesh's international banking operation and monetary reserves.

THE PARTIES

9. Bangladesh Bank is the central bank of the People's Republic of Bangladesh, established under the laws of Bangladesh and headquartered in Dhaka, Bangladesh, but which maintains the majority of its international monetary deposits in New York in an account at the New York Fed and conducts approximately eighty-five percent (85%) of its international transactions through the New York Fed.

10. Rizal Commercial Banking Corporation is one of the largest banks in the Philippines, headquartered in Makati, Philippines (a part of the Manila metropolitan area), and established and allowed the use of the numerous bank accounts necessary to the laundering and theft of the funds, including through its correspondent bank accounts at commercial banks in New York City that would serve as intermediary banks to receive, directly from the New York Fed, the Bank's stolen funds. On information and belief, RCBC maintains assets in New York, including

but not limited to those contained and/or routed through its correspondent bank accounts at the intermediary banks.

11. Maia Santos Deguito, a Philippines national, was the branch manager of RCBC's Jupiter branch, through which the stolen funds were routed.

12. Angela Ruth Torres, a Philippines national, was the Senior Customer Relations Officer of RCBC's Jupiter branch.

13. Lorenzo V. Tan, a Philippines national, at the relevant time, was the President and CEO of RCBC.

14. Raul Victor B. Tan, a Philippines national, at the relevant time, was the Head of RCBC's Retail Banking Group.

15. Ismael S. Reyes, a Philippines national, at the relevant time, was the National Sales Director of RCBC's Retail Banking Group.

16. Brigitte R. Capiña, a Philippines national, at the relevant time, was the Regional Sales Director of RCBC's Retail Banking Group.

17. Nestor O. Pineda, a Philippines national, at the relevant time, was RCBC's District Sales Director.

18. Romualdo S. Agarrado, a Philippines national, at the relevant time, was the Customer Service Head of RCBC's Jupiter branch.

19. Philrem Service Corp. is a corporation duly organized under the laws of the Philippines with a principal place of business in Makati City, Manila, Philippines and that had at the time of the theft a money transmittal license granted by the central bank of the Philippines.

20. Salud Bautista, a Philippines national, is a co-owner of Philrem.

21. Michael Bautista, a Philippines national, is a co-owner of Philrem.

22. Centurytex Trading is on information and belief a corporation duly organized under the laws of the Philippines with a principal place of business in Manila, Philippines.

23. William So Go is on information and belief a Philippines national and the owner of Centurytex Trading.

24. Bloomberry Resorts and Hotels, Inc. d/b/a Solaire Resort & Casino is on information and belief a corporation duly organized under the laws of the Philippines with a principal place of business in Manila, Philippines.

25. Eastern Hawaii Leisure Company, Ltd. d/b/a Midas Hotel & Casino is on information and belief a branch office of a Chinese corporation registered to do business in the Cagayan Special Economic Zone and Freeport Enterprise, with a principal place of business in Manila, Philippines.

26. Kam Sin Wong a/k/a Kim Wong is, on information and belief, a Philippines national, an owner of Eastern Hawaii Leisure and a signatory on one of its bank accounts.

27. Weikang Xu is, on information and belief, a Chinese national residing at an unknown address in China.

28. Ding Zhize is, on information and belief, a Chinese national residing at an unknown address in China.

29. Gao Shuhua is, on information and belief, a Chinese national residing at an unknown address in China.

30. Defendants JOHN DOES 1-25 constitute individuals and entities who may have been involved in the theft of Plaintiff's funds from its account with the New York Fed, including but not limited to personnel of RCBC, the individuals responsible for opening the accounts at RCBC in the fictitious names of Michael F. Cruz ("**Cruz**"), Jessie Christopher M. Lagrosas

("**Lagrosas**"), Alfred S. Vergara ("**Vergara**"), Enrico Vazquez ("**Vazquez**"), and Ralph C. Picache ("**Picache**," collectively with Cruz, Lagrosas, Vergara, and Vazquez, the "**Fictitious Beneficiaries**"), and any other individual or entity that was involved in the theft.

JURISDICTION AND VENUE

31. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(a) in that this action is between citizens of different states and the matter in controversy exceeds $75,000, exclusive of interest, costs, and attorneys' fees.

32. Bangladesh Bank is the central bank of the country of Bangladesh, established under the laws of Bangladesh and headquartered in Dhaka, Bangladesh. Bangladesh Bank maintains the majority of its international monetary deposits in New York in an account at the New York Fed.

33. Based on the Plaintiff's investigation, upon information and belief, none of Defendants is a citizen or resident of any of the State of New York, the United States of America, or Bangladesh.

34. This Court has personal jurisdiction over the Defendants, which engaged in a multi-national conspiracy to steal nearly a billion U.S. dollars of Plaintiff's funds from Plaintiff's account in the State of New York in New York City at the New York Fed, successfully stealing $81,001,662.12. In doing so, the Defendants struck at the heart of the global financial system by forming and carrying out a conspiracy and criminal enterprise that reached into the United States and robbed assets of Plaintiff that had been located in New York for decades and attacked the New York Fed, the very hub of the United States' participation in the international financial markets and community.

35. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because the bank account at the New York Fed that was robbed (in addition to SWIFT, by using the Fedwire system that is maintained and run by the Federal Reserve), the property that was stolen, the intermediary banks with which RCBC had, and on information and belief still has, correspondent accounts through which the stolen funds were routed and balances may be maintained, and the damages that occurred were all located in the Southern District of New York, in which this Court sits.

FACTS

I. THE HISTORY OF THE BANK AND ITS CUSTODIAL ACCOUNT AT THE NEW YORK FED IN NEW YORK CITY

A. The Bank Becomes the Central Bank of Bangladesh

36. Bangladesh achieved independence in December 1971. On November 4, 1972, Bangladesh adopted a Constitution that established the Bangladesh government as a secular, multiparty parliamentary democracy. After a period of some political upheaval and amendments to its Constitution, in 1991, Bangladesh adopted the Twelfth Amendment to its Constitution, which restored the parliamentary democratic system under which Bangladesh is governed to this day.

37. At about the same time that Bangladesh adopted its Constitution in 1972, it issued the Bangladesh Bank Order, which established the Bank as Bangladesh's central bank. The Bank is the core component of Bangladesh's financial and monetary system. It formulates and implements monetary and credit policy, regulates and supervises financial institutions, promotes development of domestic financial markets, issues currency, regulates and supervises payment systems, and acts as a banker to the government.

38. Most important, for purposes of this litigation, the Bank manages Bangladesh's international reserves.

B. The Bank's Account at the New York Fed in New York City

39. Since 1973, the Bank has held its international reserves in a custodial account in New York City with the New York Fed. This account enables the Bank to participate in the international financial system.

40. Today, Bangladesh Bank conducts approximately eighty-five percent (85%) of its international transactions in the U.S. dollar, and it does so through the Bank's custodial account at the New York Fed. On average, the Bank holds more than a $1 billion balance in the account.

41. Given the crucial importance of these reserves, the Bank has a constitutional, legal obligation as a fiduciary to the people of Bangladesh to recover the stolen funds and return them its bank account in New York City.

42. The theft of $81,001,662.12 million from its bank account in New York City caused a significant injury to the Bank and the country and people of Bangladesh. In fact, if fully successful, the theft would have taken nearly $1 billion from the Bank's account at the New York Fed, or over approximately two-thirds of the Bank's average reserves on deposit. The effects on Bangladesh, its people, and its economy could have been catastrophic.

C. The New York Fed's Role in the Domestic and International Monetary Systems

43. The Bank chose the New York Fed for its account because of the New York Fed's central role in the worldwide financial system. It provides banking and financial services to approximately 250 other foreign central banks, governments and official international institutions, such as the International Monetary Fund.

44. The New York Fed, along with the eleven other Regional Reserve Banks, the Federal Reserve Board of Governors and the Federal Open Market Committee, form the Federal Reserve System, which serves as the central bank of the United States. It works with key public

and private stakeholders "to foster the safety, soundness and vitality of our economic and financial systems." (Federal Reserve Bank of New York, What We Do, https://www.newyorkfed.org/aboutthefed/whatwedo.html.)

45. Collectively, the Federal Reserve system fulfills four overriding purposes including conducting the nation's monetary policy, supervising and regulating banking institutions, maintaining the stability of financial systems and markets, and providing financial services to major financial actors. However, each Reserve Bank within the system has independent mandates and responsibilities, and have independent corporate structures.

46. The New York Fed is unique among the Reserve Banks. It is the largest of the Regional Reserve Banks in terms of assets and volume of activity, and it intervenes in foreign exchange markets and stores monetary gold for foreign central banks, governments and international agencies.

47. One of its key missions involves the "international operations" of the Federal Reserve System. The New York Fed "intervene[s] in foreign exchange markets to achieve dollar exchange rate policy objectives and to counter disorderly conditions in foreign exchange markets," and it "acts as the primary contact with other foreign central banks." *Id.*

48. Indeed, virtually all U.S. dollar global foreign exchange transactions involving the United States government and its agencies, foreign central banks and monetary authorities with accounts at the New York Fed, and the Federal Reserve System are essentially routed through New York, and the New York Fed. This fact is critical to the New York Fed's role in maintaining the foreign exchange markets, effectuating its exchange rate policy objectives, and supporting the U.S. dollar as a global currency.

49. The New York Fed also operates Fedwire, which is developed and maintained by the Federal Reserve System and used to transfer large-dollar payments among Federal Reserve offices, depository institutions and federal government agencies. The New York Fed handles the majority of Fedwire transfers within the Federal Reserve System.

50. The Defendants and their co-conspirators usurped the Fedwire system to steal funds from the Bank's account at the New York Fed by transferring them to correspondent accounts held by RCBC at intermediary banks that were also located in New York City. Those stolen funds were then transferred from the correspondent accounts that RCBC maintained (and continues to maintain) at the intermediary banks in New York City to fictitious accounts held in the names of the Fictitious Beneficiaries at RCBC in the Philippines.

51. The conspirators took advantage of certain features of the Fedwire system and timing to accomplish their theft. Fedwire system transfers are same-day and, in many cases, instantaneous. Transferred funds are often available and final when sent. Armed with this knowledge, the conspirators sent the unauthorized payment orders after business hours at the start of the weekend in Bangladesh — which is Friday and Saturday in Bangladesh — in an attempt to effect the transfers before the New York Fed or Bangladesh Bank could discover the theft.

52. In other words, the conspirators used the New York Fed's position as a depository for the Bank's international reserves and the Fedwire funds transfer system as a critical component of their robbery. Given these facts and the New York Fed's important role in domestic and foreign monetary policy and markets, the theft of the Bank's funds out of its account at the New York Fed has vital and potentially wide-ranging consequences in the United States.

II. THE STRUCTURE OF THE CONSPIRACY TO ROB HUNDREDS OF MILLIONS FROM THE BANK'S ACCOUNT IN NEW YORK CITY

A. The North Korean Hackers Designed Their Tools and Tested Them Against Other Victims before Attacking the Bank

53. The wide-ranging conspiracy to rob hundreds of millions of dollars from the Bank began years earlier with, on information and belief, North Korean hackers. According to the FBI, among others, before the North Korean hackers executed their fraudulent transfer of funds from the Bank's New York Fed account, they first used the same or similar tools and techniques to accomplish the well-publicized attack on Sony. *See* Criminal Complaint, *United States v. Park Jin Hyok*, No. 18-MJ-1479 (C.D. Cal. June 8, 2018) ("**NK Complaint**").

54. To accomplish this, these North Korean hackers created several types of malware—software designed to infiltrate computer systems undetected—to gain access to Sony's computer systems and the other systems that they would be targeting, including the Bank's. NK Complaint ¶ 38. In particular, they created malware that would crawl from computer to computer to try to infect each computer in the chain and, if successful, transmit credentials and host information from the victim systems back to "collector" email accounts hard-coded into the malware. *Id*.

55. According to the FBI, these North Korean hackers also often used proxy techniques—anonymizing services that use the IP address of the infected computers, among others, to conceal and misrepresent the true IP address of the hacker—to mask their location and identity. *Id.* ¶ 43-44. As the FBI has observed, even knowing the domain of the IP address embedded in the malware generally "would not allow a victim or investigator to learn the location of the computer under the subjects' control," and "[t]his served to conceal evidence of their activities and intrusions." *Id.* ¶ 49.

56. The North Korean hackers put their malware to work at Sony in September 2014, engaging in internet reconnaissance and sending fraudulent spear-phishing messages—similar to what was later used to attack the Bank. *Id.* ¶ 60. The malware worked as intended, crawling across Sony's network and infecting computers and exfiltrating data along the way. *Id.* ¶ 60.

57. On November 21, 2014, after the North Korean hackers infiltrated Sony's computer system, the North Korean hackers emailed high-ranking Sony employees demanding "monetary compensation" from Sony, threatening to "bombard[]" Sony if it did not capitulate. *Id.* ¶ 62. Three days later, ransom demands with links to Sony proprietary information began popping up on computers across Sony's network. *Id.* ¶ 64-65. Several days later, the North Korean hackers sent threatening messages confirming that they had stolen information from Sony's confidential financial records. *Id.* ¶ 68.

58. The North Korean hackers accomplished this heist of credentials, data, and records by at first successfully hiding their attack by customizing the malware to engage in "a period of sustained covert reconnaissance . . . within [Sony's] network before [the North Korean hackers] launched the attack that disabled SPE's computers." *Id.* ¶ 74-75. The North Korean hackers then covered their tracks, as the malware overwrote key data making it impossible to completely trace or reconstruct the North Korean hackers' steps "through a forensic analysis." *Id.* ¶ 129.

59. Indeed, computer forensics firms including BAE Systems have reviewed the "attack toolkit" of malware used against the Bank (and then against other banks) and those firms have concluded that the malware was custom-configured to "register[] itself as a service and operate[] in an environment running SWIFT's Alliance Access software suite, [and] allow[] transactions to be deleted and records changed." Victor Mallet & Claire Jones, *Cyber thieves target bank systems after Bangladesh heist*, Financial Times, Apr. 26, 2016,

https://www.ft.com/content/8529c6a4-0b7f-11e6-9456-444ab5211a2f. In other words, the malware was designed to crawl across networks as it had successfully accomplished with Sony and then access the SWIFT systems used by banks, leaving no doubt that the intent was to target banking institutions.

60. In short, starting in 2014, well before attacking the Bank, the hackers used the same tools and techniques that they would later use on the Bank, and try to use on other banks, to infiltrate the computer systems of Sony, a multi-national, global, and sophisticated company, and steal huge amounts of data, financial information and records, credentials and user information. And they covered their tracks on the way out.

61. This was the set-up—the dry-run—for the Bank robbery.

B. RCBC—Used to Move the Stolen Funds out of the United States—Created Fictitious and Illegitimate Accounts to Begin Laundering the Money

62. The hackers also needed a bridge between the Bank's account in New York City and the Philippines casinos. That bridge was supplied by the Banking-Related Defendants.

63. RCBC was the perfect fit. It had correspondent bank accounts at commercial banks in New York City that would serve as intermediary accounts to receive, directly from the New York Fed, the Bank's stolen funds and then transfer them out of the United States to fictitious accounts set up at one of the RCBC branches in the Philippines, from which the stolen funds could be laundered.

64. The fact that the Philippines at the time did not subject the casino industry to its anti-money laundering laws (which were changed in response to the heist that is the subject of this action) made RCBC the perfect step in transferring the funds such that the Casino-Related Defendants, and other co-conspirators, would withdraw the stolen funds from the RCBC fictitious

accounts and spirit them to the Solaire Casino and Eastern Hawaii Leisure, where they would be laundered and then disappear.

65. To accomplish this step in the theft, the Banking-Related Defendants set up a number of fictitious accounts, most of which were created well in advance of the theft and then remained dormant until the conspiracy was ready to proceed.

The Obviously Illegitimate and Fictitious Accounts Created by RCBC in May 2015

66. The RCBC fictitious bank accounts in the Philippines were created by and at the behest of Defendant Wong, as well as other Doe Defendants, for the benefit of obviously fake individuals. RCBC, through senior officers and branch management, and acting within the scope of their employment and authority granted by RCBC, assisted in the opening and operation of the fictitious accounts, bypassing internal procedures and controls and choosing to ignore red flags, so that these fake accounts could lie in wait for months to receive the Bank's stolen funds.

67. Five fictitious U.S. dollar accounts were opened on May 15, 2015, almost nine months before the theft, and after the hackers had already started covert surveillance on the Bank's systems. Each was opened as an account to hold United States dollars, signaling that conspirators understood, intended, and plotted to reach into the United States—specifically into New York and the Bank's account at the New York Fed—to steal funds.

68. The first fictitious U.S. dollar account was opened in the name of Michael Francisco Cruz ("**Fictitious Cruz Account**"), a fictitious person, with a deposit of $500. It sat unused—with no transactions—until February 5, 2016 when it received $6,000,029.12 of the stolen funds. Virtually the entirety of that amount was withdrawn by February 9, 2016.

69. The second fictitious U.S. dollar account was opened in the name of Jessie Christopher M. Lagrosas ("**Fictitious Lagrosas Account**"), a fictitious person, also with a deposit

of $500. It also sat unused—with no transactions—until February 5, 2016 when it received $30,000,028.79 of the stolen funds. Approximately $22.7 million of that amount was withdrawn that same day, with almost all of the remainder withdrawn by February 9, 2016.

70. The third fictitious U.S. dollar account was opened in the name of Alfred Santos Vergara ("**Fictitious Vergara Account**"), a fictitious person, also with a deposit of $500. It also sat unused—with no transactions—until February 5, 2016 when it received a deposit of $19,999,990.00. Virtually the entirety of that amount was withdrawn by February 9, 2016.

71. The fourth fictitious U.S. dollar account was opened in the name of Enrico Teodoro Vasquez ("**Fictitious Vasquez Account**"), a fictitious person, also with a deposit of $500. It also sat unused—with no transactions—until February 5, 2016 when it received a deposit of $25,001,573.88. Virtually the entirety of that amount was withdrawn by February 9, 2016.

72. The fifth fictitious U.S. dollar account was opened in the name of Ralph Campo Picache ("**Fictitious Picache Account**," collectively with the other four accounts, the "**Fictitious Accounts**"), a fictitious person, also with a deposit of $500. It sat unused, and remained unused throughout the conspiracy, although not for lack of trying. Approximately $170 million in fraudulent payment instructions were destined for the Fictitious Picache Account but, unlike the other four Fictitious Accounts, none of the payment instructions to this account were executed by the New York Fed.

73. RCBC has since admitted that all of these accounts were fake, and established for fictitious persons, which begs the question of who could legitimately operate these accounts when there was no real owner. The answer is that the only entity that could transfer funds in and out of these accounts — which had no other owner — was RCBC itself, by and through its personnel

which, as discussed more fully below, involved multiple individuals up to the highest levels of RCBC.

74. RCBC and its senior personnel had full authority and control over these accounts, and all of the RCBC personnel who touched them, from the opening of the Fictitious Accounts, to terminating the short-lived hold, to allowing the numerous transactions to continue despite their knowledge or reckless disregard of the nature of the stolen funds.

75. The details of the opening of these Fictitious Accounts and their operations set off a virtual fireworks show of red flags and alarms that would have warned the newest of banks, much less an experienced bank like RCBC with over five decades of operations, that the accounts involved serious improprieties, as any such bank with anti-money laundering and the related "Know Your Client" ("**KYC**") procedures would have flagged. But RCBC wasn't looking for red flags. It was working with its co-conspirators.

76. The Fictitious Beneficiaries purporting to open the accounts were required to provide a driver's license. They each did. But each driver's license was fake, and even the most cursory review would have revealed this.

77. For example, the Land Transportation Office, responsible for issuing driver's licenses, had no record of Vazquez's license at all. No information from Vergara's license was even used for the account. And Lagrosas's identification had a picture of Adrian Ranas Yujuico, a reserve officer of RCBC that had worked with Deguito at her prior bank.

78. The signature specimens in each of the five account opening documents did not even match the signatures on the driver's licenses. In fact, after the theft became public, RCBC admitted in its post-hacking review that the signatures did not match.

79. The addresses and contact information in the account opening documents were wrong. When contacted after the theft, no one residing at these addresses had ever heard of the Fictitious Beneficiaries. With respect to the Fictitious Picache Account, the address listed in the account opening documents was not even an address at all, with internal RCBC documents concluding that the reason for the return of the "Thank You Letter" (discussed below) to that account was "insufficient address."

80. The account applications also indicate that the Fictitious Beneficiaries Vasquez, Vergara, and Cruz each started their "jobs" within three months of each other, eleven years earlier in 2005.

81. The account applications also claimed that each Fictitious Beneficiary worked in a "Managerial/Executive" role at actual companies. Yet even a cursory employment verification would have shown that the representations of employment at those companies were false, as RCBC's post-hacking review found.

82. In their account applications, each of the Fictitious Beneficiaries claimed that they earned an identical 1,500,000 pesos per month (approximately $28,500) at those falsified positions, with no proof of such employment or income.

83. Account opening correspondence mailed to the Fictitious Beneficiaries was returned undeliverable. In particular, RCBC compliance processes automatically send a "Thank You Letter" to the address of new account holders. But four of the five letters were returned as undeliverable between June and August 2015. RCBC learned of this and, as a matter of procedure, contacted Deguito, her supervisor, and Torres. It was then buried, and nothing further was done.

84. In fact, RCBC's policy required it to take action if a Thank You Letter is returned as undeliverable. And the business center involved must explain in a weekly report to the District

Sales Director, in this case Defendant Pineda, the action taken in response to the returned Thank You Letter. But no report was ever created.

85. In addition to Defendant Deguito, several other RCBC employees signed off on the opening of these accounts, including Torres, Erlinda Isaac, and Agarrado.

86. Upon review of Torres' computer after the theft, a word file created July 29, 2015 was found on her computer containing a draft of authorizations to open the accounts of Vazquez, Cruz, and Vergara.

87. Likewise, a security audit of RCBC's Jupiter branch after the theft uncovered in Torres' workspace a blank TIN card (a Philippines Taxpayer Identification Number card) with no picture or signature, which could have been used to fabricate the fake identification used to open the accounts.

88. According to RCBC, the account opening paperwork for the fictitious accounts was prepared and executed at a casino, businesses known in the Philippines for their involvement in money laundering. Deguito and others gave conflicting reports on whether that meeting was at the Solaire Casino. Defendant Wong testified that he and Defendant Gao executed the paperwork in Wong's office at Midas Casino (a separate casino from Solaire where one of Wong's junkets played chips purchased with the stolen funds) with Deguito present, with several other RCBC employees just outside the office. Defendant Deguito claimed as part of a Blue Ribbon Committee investigation by the Philippines Senate that she personally met the Fictitious Beneficiaries.

89. In short, the Defendants have given inconsistent stories laced with falsehoods in an effort to complicate the transactional history of the fraud and prevent the truth from being discovered.

The Other Fictitious and
Illegitimate Accounts Created by RCBC

90. Later that year, on December 8, 2015, about two months before the theft, RCBC opened accounts for each of the five Fictitious Beneficiaries. These accounts were held in the Philippine peso, not the United States dollar like the earlier Fictitious Accounts.

91. These five new fictitious accounts also came waving obvious red flags. RCBC opened the five new accounts of the Fictitious Beneficiaries with no initial deposit, unlike the fictitious U.S. dollar accounts (demonstrating that RCBC was not even bothering to get any initial deposit on any of these new accounts), and the accounts never held any funds and were never involved in any transactions. They were preparatory, opened only to be used in the event that the thieves needed additional peso accounts to distribute and launder the stolen funds. As it turned out, the accounts were not needed. The thieves were able to use other accounts, such as the Philrem and the Go-Centurytex accounts described below.

92. Later, on or around February 5, 2016, the very day on which RCBC received the stolen funds, RCBC opened yet another fictitious account—Acct. No. 9016455240—this one in the name of Defendant William So Go, doing business as Centurytex Trading ("**Go-Centurytex Account**"). The account was denominated in the United States dollar. Like everything else in connection with the conspiracy, this new account came with many red flags that RCBC chose to ignore.

93. Defendant Go never before held a United States dollar account at RCBC (only a Philippine peso account, which was opened in July 2014 and was not used in the heist). The opening of such an account on the same day that RCBC received stolen funds from the United States was highly suspicious.

94. The red flags and outright lies did not stop there. Go has since claimed inconsistently that he did not open either the U.S. dollar account or the peso account, despite that the peso account did have some level of activity before the heist. Moreover, even internal RCBC documents reveal that the signatures on the identification submitted in connection with the peso account opening did not match the specimen signature card and account opening forms, and the "Thank You Letter" sent to Centurytex Trading in connection with the peso account was returned with the stated reason "move out." If so, this is yet another fictitious account without a real owner and RCBC, as the only potential entity that had authority or control over that account and any transfers ordered into or out of such account, did not owe funds or duties to anyone but the lawful owner of the funds.

95. With respect to the U.S. dollar Go-Centurytex Account, the driver's license used to open this account did not even match the driver's license that Defendant Go had used to open the earlier Philippine peso accounts (which supposedly was of Go, although he has since claimed that the account was not his). The driver's license was a fake, so obviously so that no one could miss it. It was dated February 5, 2016, the very day on which the account was opened. Its photograph was superimposed and of shoddy quality. Its signature did not match the specimen signature on file.

96. RCBC chose to follow none of its account opening, anti-money laundering, or KYC procedures when it opened this account. It chose not to address any of the red flags, simply allowing yet another fictitious account to be opened.

97. Thereafter, the account was used (as alleged in detail below) to funnel $65.7 million from the first four fictitious accounts into other RCBC accounts, all to further the theft of tens of millions from the Bank.

98. RCBC's decisions, reaching all the way up to its highest levels, to ignore red flags time after time show that RCBC was a knowing and willing co-conspirator in the theft. In fact, even RCBC had to conclude, upon an investigation after the heist, that all RCBC personnel had "lapses and culpabilities including the District and Regional Heads."

C. The Casino-Related Defendants Further Laundered the Stolen Funds

99. North Korean persons could not then and still cannot engage in international banking due to international sanctions that severely restricted, among other things, North Korea's financial and banking capabilities. *See* Council on Foreign Relations, *What to Know about the Sanctions on North Korea*, https://www.cfr.org/backgrounder/what-know-about-sanctions-north-korea. North Korean persons cannot, on their own, steal funds from a bank account in New York City, transfer them to a bank outside of the United States, and then launder the money.

100. Therefore, the North Korean hackers would have to align with co-conspirators who could assist in moving any funds, including, in this case, on information and belief, the Bank's money to the Philippines, from which the funds could then be laundered through casinos and questionable businesses to places such as Macau, Hong Kong, or elsewhere in China where it has been widely reported that North Korean persons could circumvent international sanctions and gain access to such funds. *See* Alan Katz and Wenxin Fan, *A Baccarat Binge Helped Launder the World's Biggest Cyberheist*, Bloomberg (Aug. 3, 2017) ["**Baccarat Binge**"], https://www.bloomberg.com/news/features/2017-08-03/a-baccarat-binge-helped-launder-the-world-s-biggest-cyberheist.

101. In this case, the Philippines was not a surprising choice. The Philippines is reported to be an access point for the complex and illicit funding networks used by North Korean persons. *See* Sheena Chestnut Greitans, *Can Trump count on Manila to put pressure on North Korea? 3*

points to know., Washington Post (May 16, 2017), https://www.washingtonpost.com/news/monkey-cage/wp/2017/05/16/can-trump-count-on-manila-to-put-pressure-on-north-korea-3-points-to-know/?noredirect=on&utm_term=.0ea0c0540723.

102. At the time of the theft, the Philippines also had lax anti-money laundering laws, in particular with regard to its casino industry. *See* Nyshka Chandran, *China isn't the only country propping up North Korea*, CNBC (May 30, 2017), https://www.cnbc.com/2017/05/30/china-isnt-the-only-country-propping-up-north-korea.html. In fact, the Philippine Congress decided to strengthen those money laundering laws after the Bangladesh Bank heist to close the loopholes regarding casinos, like Solaire Casino. *See* Reuters, *Philippine Congress expands money laundering laws to include casinos* (May 30, 2017), https://uk.reuters.com/article/uk-philippines-casinos/philippine-congress-expands-money-laundering-laws-to-include-casinos-idUKKBN18Q146.

103. Furthermore, it has been reported that North Korean persons have a well-documented interest in the casino industry, which they use to launder money and evade sanctions, making the Philippines the perfect landing point for the stolen money. Joshua Hammer, *The Billion Dollar Bank Job*, N.Y. Times, May 3, 2018, https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html.

104. Moreover, certain of the Casino-Related Defendants, particularly Ding and Gao, were well versed in running (and, in Gao's case, had been convicted of running such operations in China) illegal gambling operations and foreign gaming junkets for years. They were also familiar

with Macau, a location in which North Korean persons often maintain covert bank accounts. *See* Baccarat Binge.

105. In other words, all of the necessary steps of the conspiracy were then in place and they were ready to steal the funds from the Bank's account at the New York Fed, and then launder the money and transfer it to and then out of the Philippines.

III. THE DEFENDANTS STEAL THE BANK'S MONEY FROM NEW YORK CITY

A. The Hackers Fraudulently Infiltrate the Bank's Network

106. According to the FBI, as early as October 2014, the North Korean hackers had already begun covert reconnaissance on financial institutions in Bangladesh. This was around the time that they were gearing up to attack Sony.

107. On information and belief, the conspiracy began well before that — in early 2014 or before. Indeed, Defendant Go, whose peso account at RCBC was established in July 2014, has claimed that he did not open the account, leading to the conclusion that the conspiracy had been set in motion well before then.

108. With respect to the hacking, however, by January 2015, as explained by the FBI, the North Korean hackers had specifically identified Bangladesh Bank, among other banks, as one of the targets of their attack and theft. NK Complaint ¶ 147.

109. The criminal enterprise had come together, and the co-conspirators began to open more fictitious bank accounts held in United States dollars at RCBC in the Philippines.

110. The North Korean hackers also began their spear-phishing email campaign, sending fraudulent emails to the Bank's employees misrepresenting that the fake senders were seeking employment. *Id.* ¶ 148-163. One email stated the following:

> I am Rasel Ahlam.
>
> I am extremely excited about the idea of becoming a part of your company and am hoping that you will give me an opportunity to present my case in further detail in a personal interview.
>
> Here is my resume and cover letter. Resume and cover letter [which was a link].

111. The link to the "resume and cover letter" hosted the malware that enabled the initial access to the Bank's computers. *Id.* ¶ 149.

112. The North Korean hackers also sent fraudulent spear-phishing emails to the Bank's employees appearing to be "LinkedIn" invitations. *Id.* ¶ 154.

113. Like with Sony, this is how the North Korean hackers first fraudulently gained access to those users' computers. *Id.* ¶ 164.a.

114. From there, by March 2015, the North Korean hackers had installed other forms of malware specifically designed to create a backdoor into the Bangladesh Bank network, including the colorfully named "NESTEGG," "MACKTRUCK," and "SierraCharlie," allowing the North Korean hackers to access the network, collect information, crawl across different computer systems, and then fraudulently communicate within the network over a custom binary protocol designed to appear merely as Transport Layer Security traffic. In other words, the North Korean hackers covered their tracks by using a communication protocol that misrepresents itself as authentic encrypted communications and allowed North Korean hackers to communicate the stolen data and information without tripping security alerts. *Id.* ¶ 164.b.

115. These techniques, known to the international cybersecurity and law enforcement community, were traceable only after the attack was uncovered. According to these experts, they had the hallmarks of the "Lazarus Group" and "APT38"—aliases for a group of North Korean hackers, that have been operating and honing their craft in attacks against government, finance,

and media targets since 2009, before turning their attention to banks. *Id.* ¶ 164.b; Jose Pagliery and Charles Riley, *North Korea-linked 'Lazarus' North Korean hackers hit a fourth bank in Philippines*, CNN, May 27, 2016, https://money.cnn.com/2016/05/26/technology/swift-bank-hack-philippines-lazarus/.

116. Between March 2015 and the attack in early 2016, on information and belief, the North Korean hackers gradually infiltrated Bangladesh Bank's network and performed additional covert reconnaissance on the network to gain an understanding of the specific systems needed for the cyberattack as well as information that would be helpful in executing the cyberheist. NK Complaint ¶ 164.b-c.

117. Finally, on January 29, 2016, only six days before the theft, the hackers began to covertly move across the Bangladesh Bank network, from the computers in which they had originally installed the malware, to the SWIFTLIVE system critical to the processing of SWIFT messages like those used to execute the heist. *Id.* ¶ 164.c-d.

118. Continuing to hide their presence, the North Korean hackers then reached the SWIFT Alliance Access application, a customer-managed gateway to the SWIFTLIVE network that transmitted and received the SWIFT messages used to create and confirm financial transactions. The hackers covered-up their various attempts to log on to that system and laid in wait until they were ready to execute the heist. *Id.* ¶ 164.c-d.

B. The Hackers Sent Unauthorized Payment Orders to the New York Fed

119. The robbery was set into motion on Thursday, February 4, 2016 after the close of business in Bangladesh. This was just before a holiday weekend in the Philippines for which RCBC was closed the following Monday, February 8, for the Chinese New Year. The conspirators

took advantage of this, as well as the time zone differences between New York (GMT-5), Bangladesh (GMT+6), and the Philippines (GMT+8).

120. In particular, the Bangladesh work week runs from Sunday through Thursday, with Friday and Saturday as the weekend. As a consequence, by waiting to access the system until after the close of business on Thursday and initiating the fraudulent payment orders that evening, the North Korean hackers were attempting to minimize the likelihood of being caught over the weekend in Bangladesh (and the long weekend from Saturday to Monday in the Philippines).

121. Similarly, by sending the fraudulent payment orders on Thursday night, the North Korean hackers ensured that the payment orders would reach New York by Thursday morning New York time. This would enable the New York Fed, and the various intermediary banks that were also located in New York, to process the transactions on Thursday, February 4 in New York (when it was the start of the weekend in Bangladesh) and to deliver the stolen funds to the fraudulent RCBC accounts.

122. Therefore, as soon as Bangladesh Bank closed for the weekend, the North Korean hackers got to work.

123. The malware that they had installed and that had been designed to hide itself from the Bank worked as thieves had planned and granted them unauthorized access to the Bank's systems. The North Korean hackers were able to log into the SWIFT system at approximately 8:36 p.m. and began to create fraudulent payment instructions to execute the heist. Starting at approximately 8:55 p.m. through approximately 10:30 p.m. (which was 9:55 a.m. to 11:30 a.m. in New York on Thursday, February 4), the hackers sent 36 fraudulent payment orders for nearly $1 billion—intended to drain the bulk of the Bank's account at the New York Fed.

124. Only one of these payment orders, however, contained the intermediary bank routing information that was necessary to process the transaction. That payment order was for $20 million and was to be routed from the New York Fed, through an intermediary bank to the "Shalika Fundation" in Sri Lanka. Ultimately, the Sri Lankan bank that received that payment order—the Pan Asia Banking Corporation—flagged it because it misspelled the word "Foundation" as "Fundation" and because the size of the transaction was unusual, causing personnel at that bank to flag the transaction for review (and subsequently return those funds to the Bank).

125. The other 35 payment orders were rejected by the New York Fed for their lack of intermediary bank information, and the hackers quickly updated the payment orders with the necessary intermediary bank information and resent them — but only 34 of them, omitting one of the payment instructions in their haste — between approximately 11:30 p.m. on February 4 and 1:00 a.m. on February 5, Bangladesh time (or 12:30 p.m. to 2:00 p.m. New York time on Thursday, February 4).

126. Satisfied that they had successfully sent the updated payment instructions, that the intermediary bank information for RCBC's correspondent banks had been accepted, the hackers logged out of the SWIFT system at 3:59 a.m., at which point the malware they had designed to cover their tracks kicked in and started deleting key files that would allow anyone at the Bank to easily uncover what the hackers had done, even including disabling a SWIFT printer that would normally print such payment instructions for the Bank's records.

127. Ultimately, four of the unauthorized payment orders were fully executed.

IV. THE DEFENDANTS USED RCBC'S CORRESPONDENT BANK ACCOUNTS TO TRANSFER THE STOLEN FUNDS OUTSIDE OF THE UNITED STATES

128. RCBC did not have an account with the New York Fed. Accordingly, as noted above, to be able to steal the Bank's funds from its New York Fed account and transfer them out

of the country to RCBC in the Philippines, the thieves had to use intermediary banks at which RCBC did have correspondent accounts.

129. RCBC had, and on information and belief continues to have, such a relationship with at least three banks: Wells Fargo; Bank of New York Mellon; and Citibank. Each of these banks has a New York location at which RCBC has a correspondent account through which the thieves could route the stolen funds, and which, on information and belief, may also contain balances in addition to their use to route funds out of the United States. Each of those New York intermediary banks also had relationships with the New York Fed. Therefore, they could use Fedwire to immediately receive the stolen funds from the New York Fed and then transfer them, without delay, to RCBC in the Philippines on the same business day.

130. This was critical to the conspirators' plan to transfer the funds into the RCBC accounts by or before February 5, 2016, so they could ensure their co-conspirators were ready to execute the plan, and begin to drain the accounts and launder the stolen money before the end of Bangladesh's weekend.

131. In short, RCBC's correspondent bank accounts maintained in New York City with three intermediary banks were critical to moving the stolen funds out of the United States to RCBC in the Philippines and doing so quickly, so that the funds could be distributed and laundered before the theft was detected or efforts to retrieve the stolen funds could be successful.

132. Those were precisely the accounts that the hackers would use to deliver the funds to RCBC so they could be laundered.

133. The first executed unauthorized payment order in the amount of $6,000,039.12 was sent from the Bank's account at the New York Fed in New York City at 11:26 p.m. on February 4, 2016 Bangladesh time (12:26 p.m. on February 4 in New York). The stolen funds, however,

were first transferred to RCBC's correspondent account at the offices of Wells Fargo Bank, N.A. (the intermediary bank) in New York City (SWIFT code PNBPUS3NNYC), from which they were transferred out of the country to the Fictitious Cruz Account at RCBC in the Philippines.

134. The second executed unauthorized payment order in the amount of $30,000,039.12 was sent from the Bank's account at the New York Fed in New York City at 11:59 p.m. on February 4, 2016 Bangladesh time (12:59 p.m. on February 4 in New York). The stolen funds, however, were first transferred to an RCBC correspondent account, this one at the offices of the Bank of New York Mellon (the intermediary bank) in New York City (SWIFT code IRVTUS3N), from which they were transferred out of the country to the Fictitious Lagrosas Account at RCBC in the Philippines.

135. The third executed unauthorized payment order in the amount $20,000,000.00 was sent from the Bank's account at the New York Fed at 12:00 a.m. (midnight) on February 5, 2016, Bangladesh time (1:00 p.m. on February 4 in New York). The intermediary bank was Wells Fargo Bank, N.A.'s Philadelphia office, SWIFT code PNBPUS33, from which the stolen funds were transferred to the Fictitious Vergara Account at RCBC in the Philippines.

136. The fourth executed unauthorized payment order in the amount $25,001,583.88 was sent from the Bank's account at 12:02 a.m. on February 5, 2016, Bangladesh time (1:02 p.m. on February 4 in New York). The stolen funds, however, were first transferred to RCBC's correspondent account at the offices of Citibank, N.A. (the intermediary bank) in New York City (SWIFT code CITIUS33), from which they were transferred out of the country to the Vazquez account at RCBC in the Philippines.

V. WITH THE STOLEN FUNDS NOW IN THE PHILIPPINES, RCBC AND DEFENDANTS BEGAN LAUNDERING THE STOLEN FUNDS THROUGH FICTITIOUS AND ILLEGITIMATE ACCOUNTS

A. The Conspirators, Including Senior RCBC Personnel, Were Ready and Waiting to Launder the Stolen Funds Once They Arrived

137. On February 5, 2016, the day that the stolen funds arrived in the Philippines, the Defendants were actively monitoring the Fictitious Accounts—waiting for them to arrive. Between 11:30 a.m. and 12:00 p.m., Wong—clearly knowing that the stolen funds were coming—called Deguito and asked whether a large deposit had been transferred into the Fictitious Cruz Account. Deguito checked, and a large deposit *had* arrived—approximately $6 million.

138. When Deguito asked Wong how he knew that the funds were coming, Wong told her, "I told you, Lorenzo [Tan] knows this." Deguito was not surprised. Lorenzo Tan, RCBC's President and CEO, was a close friend of Kim Wong, and Lorenzo Tan had previously told Deguito to "take care of" Wong as a client of RCBC. In fact, Lorenzo Tan admitted to the Senate Blue Ribbon Committee that Kim Wong had been a "social acquaintance" since 2002.

139. Wong called Deguito several more times that day, arranging for the use of Philrem's RCBC accounts to launder the stolen funds. Deguito obliged, as later did numerous RCBC officials who—motivated by the prospect of significant fees and commissions for RCBC, including in foreign exchange transactions with the RCBC Treasury, which Michael Bautista had already started conducting—used their positions to remove a hold that had momentarily been placed on the Fictitious Accounts and to delay the implementation of stop payment instructions.

140. Later, before the Philippine Senate's Blue Ribbon Committee, Deguito testified that Lorenzo Tan knew about the opening of the Fictitious Accounts, but chose to do nothing. On May 6, 2016, after the robbery, Lorenzo Tan had to resign as RCBC's President and CEO, claiming that he was taking "full moral responsibility" but was innocent.

B. RCBC Accepted the Stolen Funds into the Fictitious Accounts

141. All of this was highly suspicious given that the Fictitious Accounts, which had been opened nearly nine months earlier, had never been involved in a single transaction. They were not even in Wong's name.

142. The managers and officials at RCBC, knowing that RCBC stood to profit substantially in fees and commissions in connection with the laundering of these stolen funds, chose to ignore, as long as necessary, the suspicious nature of the Fictitious Accounts and the tens of millions of dollars that were suddenly laundered through them.

The Fictitious Cruz Account

143. For example, from the moment it was opened on May 15, 2015 until February 5, 2016, almost nine months later, the Fictitious Cruz Account had absolutely no activity. Then, when the robbery happened, it suddenly became active, receiving and distributing massive amounts of money. Beginning on February 5, 2016, the following transactions occurred, all involving the stolen funds:

Table 4

Txn Date	Debit Amt. (USD)	Credit Amt. (USD)	Balance (USD)
02/05/16		6,000,029.12	6,000,529.49
02/05/16	3,755.02		5,996,774.47
02/09/16	**5,985,883.47**		10,891.00
02/12/16	10,891.00		0.00

144. The $6,000,029.12 credit on February 5, 2016 listed in this table is the arrival of the stolen funds laundered and routed through RCBC's correspondent account at Wells Fargo in New York. The fraudulent payment instruction described this massive payment as a (fake) consultant fee to Cruz for something called the "IPFF Project Cell Bangladesh." The $3,755.02 debit listed in the table are fees paid to RCBC with the stolen funds. The other two debits are transfers of the stolen funds out of the account (with a small transfer of $10,891 back to the Bank).

This one week eruption of receipts and transfers of massive amounts money was the only activity ever to happen in this account after it was opened nearly nine months earlier.

The Fictitious Lagrosas Account

145. The Fictitious Lagrosas Account also had absolutely no activity since it was opened on May 15, 2015. Then, for one week, from February 5 to 12, 2016, it had the following transactions in the tens of millions of dollars, all involving the stolen funds:

Table 5

Txn Date	Debit Amt. (USD)	Credit Amt. (USD)	Balance (USD)
02/05/16		30,000,028.79	30,000,529.16
02/05/16	18,755.02		29,981,774.14
02/05/16	**22,735,000.00**		7,246,774.14
02/09/16	**7,236,154.62**		10,619.52
02/12/16	10,619.52		0.00

146. This table shows a February 5, 2016 transfer of $30,000,028.79, which is the arrival of the stolen funds laundered through RCBC's correspondent account at Bank of New York Mellon in New York City. The fake purpose of this massive payment listed in the fraudulent payment instruction was "Dhaka Mass Rapid Trans. Dev. Proj." The debit of $18,755.02 on that same day represents RCBC fees paid from the stolen funds. The next two debits are transfers and laundering of over $30 million of the stolen funds out of the account, with the final debit of $10,619.52 being a transfer back to the Bank after this Fictitious Account had essentially been emptied. This one week laundering of over $30 million was the only activity to happen in an account that was opened nearly nine months earlier.

The Fictitious Vergara Account

147. The story is the same with the Fictitious Vergara Account. It had no activity after it was opened on May 15, 2015, until almost nine months later. Then, on February 5, 2016, the following transactions occurred, all involving the stolen funds:

Table 6

Txn Date	Debit Amt. (USD)	Credit Amt. (USD)	Balance (USD)
02/05/16		19,999,990.00	20,000,490.37
02/05/16	12,504.99		19,987,985.38
02/09/16	**19,951,502.13**		36,483.25
02/12/16	36,483.25		0.00

148. The February 5, 2016 credit of $19,999,990.00 represents funds stolen from the Bank and laundered through RCBC's correspondent account at Wells Fargo in Philadelphia. The fake reason provided for this payment in the fraudulent payment instruction was "Engineering Consulting Fees, Application No. 16FCE" in connection with the "Bheramara Combined Cycle Power Plan Development Project." The $12,504.99 debit on the same day represents fees paid to RCBC from the stolen funds. The February 9, 2016 debit of almost all of the remainder of the stolen funds represents further laundering of the stolen funds through accounts held at RCBC, and the debit of a mere $36,483.25 is the return of stolen funds to the Bank.

The Fictitious Vasquez Account

149. The Fictitious Vasquez Account had the same type of highly suspicious activity over the same time period. In particular, it had no activity whatsoever from its opening on May 15, 2015 until February 5, 2016. Then a massive amount totaling over $25 million of stolen funds was transferred into the account, only to be laundered out of the account in just one week:

Table 7

Txn Date	Debit Amt. (USD)	Credit Amt. (USD)	Balance (USD)
02/05/16		25,001,573.88	25,002,074.25
02/05/16	15,630.98		24,986,443.27
02/09/16	**15,215,977.26**		9,770,466.01
02/09/16	**9,760,124.15**		10,341.86
02/12/16	10,341.86		0.00

150. The February 5, 2016 credit of $25,001,573.88 represents stolen funds spirited and laundered out of the United States through RCBC's correspondent account at Citibank in New York City. The fake reason for the payment listed in the fraudulent payment instruction was "The

Kanchpur, Megna and Gumti 2nd Bridges Const. Project, Govt. of the People's Republic of Bangladesh." The debit of $15,630.98 on the same day represents fees paid to RCBC from the stolen funds. The two debits on February 9, 2016 of almost $25 million are further laundering of the stolen funds through accounts held at RCBC. The February 12, 2016 debit of $10,341.86 is the relatively meager return of stolen funds to the Bank.

C. Nervous That a Hold Might Be Placed on the Fictitious Accounts, RCBC Personnel Acted Quickly to Begin Laundering the Stolen Funds

151. On the afternoon of February 5, 2016, with the stolen funds now held in the Fictitious Accounts, Michael Bautista of Philrem immediately began to try to launder them and transfer them to other accounts at RCBC, including through foreign exchange transactions with RCBC's Treasury through which RCBC profited handsomely.

152. At 2:51 p.m., Michael Bautista asked RCBC's Treasury Department, in particular trader Jennifer M. Ona, to purchase Philippine pesos and deposit them in a peso account at RCBC's Pasig branch by using $13,500,000 from the Fictitious Lagrosas Account. After learning from Ona that a peso account in RCBC's Pasig branch was not yet available, Michael Bautista quickly changed plans, deciding instead to use Philrem's peso account at RCBC's Unimart branch (where Philrem also had a dollar account) to receive the stolen funds converted to pesos.

153. The Bautistas, however, did not want to transfer the stolen funds directly into an account held by Philrem, their company. They wanted the transfer to be indirect, through a middle-man account, to add a layer of deniability for Philrem (and RCBC).

154. Defendant Deguito quickly sprang into action. Around 3:00 p.m., only nine minutes after Michael Bautista first started the process of laundering the funds through RCBC's Treasury, Deguito rapidly processed the opening of the Go-Centurytex Account. About thirteen minutes later, at 3:13 p.m., a massive amount of money—$22,735,000 of the $30,000,028.79 of

the stolen funds, which had just been deposited into the Fictitious Lagrosas Account—was transferred to Go-Centurytex Account, which had existed for all of 13 minutes.

155. Given that Lagrosas was an account holder who never existed in the first place, and the Go-Centurytex Account was fashioned out of whole cloth in a matter of minutes, there were no real parties to this laundering transaction. RCBC, however, falsely papered the transaction as a cash withdrawal rather than a funds transfer ostensibly to prevent anyone from attempting to call it back not realizing it was only a funds transfer from the fictitious Lagrosas. The withdrawal slip lists Deguito as approving the transaction, Torres reviewing it, and Lagrosas (who did not exist) receiving the cash (which makes no sense given that RCBC's Jupiter branch did not have that much cash on hand, as was made plain by the branch's requests for 20 million pesos from a different branch later in the day, as discussed below). All of their signatures, including the fictitious Lagrosas signature, appear on the withdrawal slip. The withdrawal slip contained a written note stating that the funds were to be deposited in the Go-Centurytex Account: "TF to 9016455240."

156. With this go-between transaction accomplished, the thieves started shifting the stolen funds to Philrem's peso account at RCBC's Unimart branch. But, first, to further complicate the money trail, they transferred the stolen funds to Philrem's dollar account at the Unimart branch. Specifically, at 3:27 p.m., that account received a transfer of $14,200,000 of the stolen funds from the newly minted Go-Centurytex Account. At 4:48 p.m., they transferred an additional $500,000. Only then did they move these stolen funds to Philrem's peso account. In particular, at 5:47 p.m. and 5:49 p.m., respectively, RCBC's Unimart Branch debited $13,500,000 and $500,000 to Philrem's dollar account and credited 644,220,000 and 3,810,000 pesos to Philrem's peso account.

157. This multi-step process of the money laundering had now been accomplished. On information and belief, RCBC received substantial fees for the transfer and foreign exchange of these stolen funds between these accounts.

158. Indeed, the pesos ultimately deposited in Philrem's peso account at RCBC's Unimart branch were the result of Philrem's trading dollars for pesos with the Treasury Department:

Date	**Time**	USD (in Millions)	**Rate (Php)**	Php (in Millions)	**Trader**
02.05.16	4:18:31 p.m.	13.5	47.72	644.220	J.M. Ona/1
02.05.16	4:19:59 p.m.	0.5	47.62	23.810	J.M. Ona/2

On information and belief, RCBC earned substantial fees and commissions on these multi-million dollar trades.

159. To even further complicate the money trail, around the same time, between 3:33 p.m. and 5:49 p.m., RCBC personnel and Philrem used certain of the stolen funds that had been shifted into the newly minted Go-Centurytex Account and then quickly moved through the Philrem U.S. dollar account (at 3:27 p.m. and 4:58 p.m.) and then into the Philrem peso account (at 5:45 p.m. and 5:49 p.m.) — 655,005,000 pesos or approximately $12.46 million in total — to purchase five managers checks worth 635,000,000 pesos that listed Philrem as the payee. Those manager's checks were then given to Salud Bautista, who deposited them back into Philrem's other accounts at other banks Banco de Oro Unibank, Inc. ("**BDO**") and Metropolitan Bank and Trust Company ("**Metrobank**").

160. These laundering transactions all happened in less than an hour.

161. The conspirators, however, still remained concerned that the suspicious transactions would be discovered and a hold would be placed on the accounts. So, before that happened, they decided to take cash from the Go-Centurytex Account and abscond with it.

162. They had a problem, though. RCBC's Jupiter branch did not have enough cash on hand to pay-out these cash withdrawals.

163. The conspirators had a work-around. They requested a delivery of 20 million pesos in cash (approximately $380,000) from another branch, RCBC's Makati Cash Center. That delivery arrived via hand-delivery before 7:00 p.m. that night. As it turns out, this delivery came just in time, as only minutes later certain RCBC personnel actually did place a hold—even if only momentarily—on the Fictitious Accounts.

164. With 20 million pesos in hand, Deguito and Torres put the money in "a cardboard box" and held it "while waiting" for the mysterious William So Go to come pick it up. Of course, keeping this cash in a cardboard box and out of the computer systems of the bank would ensure that any hold placed on the accounts would not affect RCBC personnel's ability to launder that cash.

165. Shortly thereafter, Torres claimed that she saw William So Go (pointed out by Deguito) drive into the parking lot in a dark gray Lexus and roll down his window. She gave him the cash. Torres had to override the bank's systems simply to hand over such a large amount of cash, which exceeded RCBC's teller limit. Torres claimed, later, that she reviewed the identification documents for So Go on file at RCBC and determined that the picture in the file was a different person from the one to whom she handed the cash. But, in truth, she already knew. A handwriting expert confirmed that Torres had earlier written the entries on the "Customer Relation Form (CRF)" of So Go's account, presumably when he opened it.

166. Setting aside that much of Torres's story is not believable on its face, security guards on site at RCBC's Jupiter branch said that, in fact, a messenger carried the box of cash outside of the bank, not Torres. They also said that the box of money was not given to So Go. It was placed in Deguito's car.

167. The RCBC personnel also tried to hide evidence of their illicit activity. The Jupiter branch's closed circuit television system ("**CCTV**") was conveniently not working from February 4 to February 9, 2016—the very time period during which the stolen funds were laundered. A subsequent investigation determined that "the timing of the damage to the CCTV [was] suspicious" and "that it was tampered" with.

168. The falsehoods and inconsistencies of the RCBC personnel with regard to this money laundering is further evidence that senior management at RCBC, including senior officials in multiple branches, knew about and/or condoned the theft and the effort to distribute and launder the money.

D. A Hold Was Placed on the Fictitious Accounts, but RCBC Management Quickly Removed It, Allowing the Stolen Funds to Be Further Laundered

169. As it turned out, the efforts of RCBC personnel to quickly launder the funds after they arrived on Friday, February 5, 2016, were not entirely necessary. While a hold was placed on the Fictitious Accounts later that day in the early evening, about 45 minutes after the hold was put in place RCBC senior management removed it. This allowed tens of millions of dollars of the Bank's stolen funds remaining in the Fictitious Accounts to be completely looted and laundered when the bank opened for business on the Tuesday after the holiday weekend.

170. With regard to the hold that was momentarily put in place on Friday, February 5, 2016 that process started with an Operations Manager at RCBC's Settlements Department Florentino Requinta. She saw the suspicious transfers into the previously inactive Fictitious

Accounts and escalated her concerns as the start of a process that eventually reached RCBC District and Regional Levels.

171. Specifically, Requinto sent a 5:49 p.m. email notifying Merci Cuaresma and Edgar Miguel, the Division and Department Heads, respectively, of RCBC's Cash Management Services Division. Cuaresma reviewed the transactions, determined that they were suspicious and notified Sabino Maximiano Eco, the Deputy Head of RCBC's Operations Group, who then notified his boss, Dennis Bancod, the Head of RCBC's Operations Group, and Nancy Quiogue, the Regional Sales Head of RCBC's Service Group.

172. As a result, RCBC placed a hold (which turned out to be temporary) on the Fictitious Accounts and the Go-Centurytex Account. Eco asked Richard lnsigne, the Head of RCBC's Core Banking System, to put the hold in place, and it was posted sometime between 6:45 p.m. and 7:04 p.m.

173. Even before Eco asked that the hold be put in place, RCBC's process to remove that hold had begun.

174. In particular, Raul Victor B. Tan, who had recently stepped down from his position as Head of the Retail Banking Group, determined that the propriety of the hold should be discussed. He contacted senior personnel in RCBC's Sales Department, in particular Pineda and Capiña, the District and Regional Sales Directors. They then chose to consult with Deguito, who told them that the account holders were long-time, wealthy clients from the Solaire Casino whose account documents were "in order" and that the transfers had been expected.

175. Then Raul Tan, despite having learned about the suspicious transactions from Eco, ordered the hold to be lifted. The hold was then lifted between 7:29 p.m. and 7:30 p.m., only about 45 minutes after it was put in place.

176. Capiña later asked about the hold by text message to Eco at or around 7:59 p.m. apparently not having heard that Raul Tan ordered it lifted. Eco replied that the decision was "not to hold acct per Rbts [Raul Tan's] advice. Maia will just report STR." In other words, there was no need to keep a hold in place even though a suspicious transaction report ("**STR**") would be filed. Of course, by the time any STR was finalized, it was three days later and the funds were long gone.

177. These inexplicable actions by senior RCBC personnel indicate that they had knowledge of the tainted source of the funds.

178. In fact, after Raul Tan was informed that the Bank had requested that the funds be recalled, he stated that it was "Bangladesh's problem," not RCBC's problem.

179. Moreover, Raul Tan made this decision as to whether to release the hold even though he was no longer Head of the Retail Bank Group and had no authority to do so. The decision should have been made by Ismael Reyes, whom Raul Tan designated the Officer-in-Charge of Retail Banking after he stepped down. Reyes chose not to make the decision, though. His inaction was even more suspicious given that RCBC's own internal documents demonstrate that RCBC, including Reyes and other senior bank officials, should have foreseen potential issues and exercised even a modicum of diligence given RCBC's knowledge that RCBC's Jupiter branch had recently been involved in similar suspicious transactions involving a fraudulent $1 billion HSBC check.

180. Instead, Raul Tan made the decision, and Reyes, Capiña, Pineda, and other senior RCBC officials never questioned it.

181. With this, RCBC allowed the theft and laundering of the stolen funds to continue and ultimately be completed starting the morning of the next business day, and RCBC continued to earn substantial fees and commissions on the subsequent trading and transfers.

182. This history further evidences senior RCBC management's involvement in and knowledge of the theft and money laundering, and/or reckless disregard for the rights of the Bank.

183. Indeed, even after it was completely clear to any objective observer that the funds were stolen, RCBC made no effort to stop the payments or claw them back from other RCBC accounts into which they were transferred, allowing such transactions to occur – as described below – on February 10 through 12, even after RCBC admitted to having received the stop payment requests from the Bank.

184. Despite that these individuals were all acting pursuant to powers they had been granted by RCBC (except Raul Tan who apparently did not have the authority to release the hold at that time), senior officials at RCBC elected to exercise zero control or authority over any personnel from Deguito and Torres up to senior personnel at RCBC's Head Office. This is despite the fact that the fraudulent nature of the transactions and deposits were entirely apparent, and the laundering of the funds completely foreseeable — indeed, that is why there is an entire area of anti-money laundering laws, rules, and policies internationally, in the Philippines, and even at RCBC (which RCBC personnel completely ignored).

E. The Next Business Day, RCBC received the Bank's Stop Payment Notices but Delayed Their Implementation to Allow the Remainder of the Stolen Funds in the Fictitious Accounts to Be Looted and Laundered

185. On Monday, February 8, 2016, the Bank sent SWIFT messages (between 5:05 p.m. and 5:12 p.m., Bangladesh time) to RCBC requesting RCBC to (i) stop payment to three of the

Fictitious Accounts—in particular, the Fictitious Vazquez, Vergara, and Lagrosas Accounts and (ii) freeze the accounts, if payment had already been made.

186. The first stop payment request, with respect to the Fictitious Vazquez Account, sent Monday, February 8, was sent with the phrase "STOPPAY" in the reference and contained the following narrative:

> TOP URGENT……..TOP URGENT……..TOP URGENT
> .
> .
> REF TO THE TRANSACTION VALUE DATE 160204, AMOUNT USD 25,001,583.88, BENEFICIARY: ENRICO T. VAZQUEZ, 70 JUPITER STREET, BEL-AIR VILLAGE, MAKATI CITY, A/C NO: []. PLEASE BE INFORMED THAT THIS IS A DOUBTFUL TRANSACTION. YOU ARE REQUESTED TO STOP THE PAYMENT AND IF YOU HAVE ALREADY MADE THE PAYMENT THEN FREEZE THE ACCOUNT OF BENEFICIARY FOR PROPER INVESTIGATION. WE THINK THE TRANSACTION IS CONTRADICTORY WITH THE ANTI MONEY LAUNDERING LAW.
> .
> WE ALREADY ASKED [THE INTERMEDIARY BANK] TO CALL BACK THE FUND. PLEASE FEEL FREE TO CONTACT US FOR FURTHER QUERY.
> .
> YOUR COOPERATION IN THIS REGARD WILL BE HIGHLY APPRECIATED.

187. The second stop payment request, with respect to the Fictitious Vergara Account, sent Monday, February 8, was sent with the phrase "STOPPAY" in the reference and contained the following narrative:

> TOP URGENT……..TOP URGENT……..TOP URGENT
> .
> .
> REF TO THE TRANSACTION VALUE DATE 160204, AMOUNT USD 20,000,000.00, BENEFICIARY: ALFRED S. VERGARA, 1 HUMABAN STREET, G/F VALERO CARPARK 2, VALERO STREET, SALCEDO VILLAGE, MAKATI CITY, A/C NO: []. PLEASE BE INFORMED THAT THIS IS A DOUBTFUL TRANSACTION. YOU ARE REQUESTED TO STOP THE PAYMENT AND IF YOU HAVE ALREADY MADE THE PAYMENT THEN FREEZE THE ACCOUNT OF BENEFICIARY FOR PROPER

INVESTIGATION. WE THINK THE TRANSACTION IS CONTRADICTORY WITH THE ANTI MONEY LAUNDERING LAW.
.
WE ALREADY ASKED [THE INTERMEDIARY BANK] TO CALL BACK THE FUND. PLEASE FEEL FREE TO CONTACT US FOR FURTHER QUERY.
.
YOUR COOPERATION IN THIS REGARD WILL BE HIGHLY APPRECIATED.

188. The third stop payment request, with respect to the Fictitious Lagrosas Account, sent Monday, February 8, was sent with the phrase "STOPPAY" in the reference and contained the following narrative:

TOP URGENT……..TOP URGENT……..TOP URGENT
.
.
REF TO THE TRANSACTION VALUE DATE 160204, AMOUNT USD 30,000,039.12, BENEFICIARY: JESSIE CHRISTOPHER M. LAGROSAS, 1 HUMABON STREET, MAGALLANES VILLAGE, MAKATI CITY, A/C NO: []. PLEASE BE INFORMED THAT THIS IS A DOUBTFUL TRANSACTION. YOU ARE REQUESTED TO STOP THE PAYMENT AND IF YOU HAVE ALREADY MADE THE PAYMENT THEN FREEZE THE ACCOUNT OF BENEFICIARY FOR PROPER INVESTIGATION. WE THINK THE TRANSACTION IS CONTRADICTORY WITH THE ANTI MONEY LAUNDERING LAW.
.
WE ALREADY ASKED [THE INTERMEDIARY BANK] TO CALL BACK THE FUND. PLEASE FEEL FREE TO CONTACT US FOR FURTHER QUERY.
.
YOUR COOPERATION IN THIS REGARD WILL BE HIGHLY APPRECIATED.

189. But when the Bank sent these SWIFT messages, RCBC was not logged onto its SWIFT server. That was because the day before, Sunday, February 7—a weekend day—someone logged RCBC off of the SWIFT Server at 6:54 a.m. RCBC personnel only logged back onto the SWIFT Server at 9:11 a.m. on Tuesday, February 9.

190. On information and belief, Deguito herself would not have had access to such a system, which is a critical component of a bank's foreign transactions. Such an important system would only be accessible to critical staff, likely in RCBC's Head Office.

191. Given this highly suspicious timing and the fact that RCBC personnel were aware that the payment instructions were delivered through SWIFT and so any stop payment instructions would likewise be delivered through SWIFT, on information and belief, someone at RCBC, acting with the authority that their scope of employment provided them with respect to the critical SWIFT server, logged the system off to prevent the receipt and review of the stop payment instructions.

192. Accordingly, RCBC did not review the stop payment and hold messages until Tuesday, February 9, 2016 at 9:11 a.m. Orlando de la Cruz of RCBC's Settlement Department forwarded the SWIFT messages to his supervisor, Jose P. Mesina, Jr. and officers at RCBC's Jupiter branch, including Deguito, Torres, and the Head of Customer Service, Romualdo S. Agarrado.

193. The messages were then escalated to many of the same Senior RCBC personal, who were involved in the process four days earlier that quickly canceled the "hold" on these same Fictitious Accounts, including Quiogue, Raul Tan, Racela and Reyes. *Id.* at ¶ 54.

194. RCBC's Settlements Department claimed that they began forwarding the Bank's SWIFT messages to RCBC's Jupiter Branch at 10:59 a.m. on February 9, 2016. These actions, however, did nothing more than alert the RCBC personnel at that branch to restart their laundering of the stolen funds out of the Fictitious Accounts. RCBC's Settlements Department apparently did nothing themselves to place a hold or freeze on those accounts.

195. RCBC personnel then jumped into action to continue transferring funds out of the Fictitious Accounts, which, again, could not have been drained by anyone but RCBC given RCBC's own admission that the accounts were fictitious.

196. In all, they withdrew approximately $58.2 million of the Bank's stolen funds from the Fictitious Accounts—essentially draining them completely—and deposited $42.9 million into the Go-Centurytex Account and $15.2 million into the Philrem account at RCBC's Unimart branch. Torres approved these withdrawals and deposits.

197. In particular, at 10:24 a.m., $15,215,977.26 was moved from the Fictitious Vasquez Account to a Philrem account. These funds were later shifted to the Go-Centurytex Account and then an account held by Defendant Philrem.

198. At 11:19 a.m., $19,951,502.13 was moved from the Fictitious Vergara Account to the Go-Centurytex Account.

199. At 11:34 a.m., $9,769,124.15 was moved from the Fictitious Vasquez Account to the Go-Centurytex Account and Philrem's account at RCBC's Unimart branch office. The funds transferred to the Go-Centurytex Account would also be subsequently transferred to the same Philrem account.

200. At 11:35 a.m., $7,236,154.62 was moved from the Fictitious Lagrosas Account to the Go-Centurytex Account.

201. Finally, at 11:37 a.m., $5,985,883.47 was moved from the Fictitious Cruz Account to the Go-Centurytex Account.

202. Given that the holders of each of these Fictitious Accounts did not exist, there is no real evidence that an account holder ordered these withdrawals, which leaves only RCBC as the entity with any authority over these Fictitious Accounts. Deguito and Torres signed the withdrawal

slips. And, as already alleged, during this time RCBC's closed circuit television was not operating and so there is no video of any withdrawals from these Fictitious Accounts.

203. By 11:37 a.m., less than an hour after RCBC forwarded the SWIFT messages to the Jupiter branch *but did nothing else*, the Fictitious Accounts had been drained to $10,341.86 (Vasquez), $10,891 (Cruz), $10,619.52 (Lagrosas), and $36,483.25 (Vergara).

204. If RCBC, including RCBC senior management, had simply chosen to place a hold or freeze on those Fictitious Accounts upon receiving the SWIFT message, it could have prevented the transfer of most of the remaining funds out of those accounts. Instead, it in essence alerted other RCBC personnel that the Bank was seeking the return of its stolen funds.

205. Setting aside that RCBC could have put a hold back onto this account—the very same hold that it had removed after 45 minutes on Friday night—it could have just as easily frozen the RCBC accounts to which the stolen funds had just moved. And many of those stolen funds sat in those other accounts for days. Instead, RCBC chose to allow the stolen funds to continue to be looted and laundered.

206. Indeed, to the extent RCBC has claimed, as discussed more fully below, that it was hamstrung by bank secrecy laws or bank policy, not only had RCBC already shown itself completely willing to wholly disregard any such policies, but RCBC has admitted that the accounts were all fictitious. No one but RCBC could have objected to the placement of such a freeze or return of the stolen funds to those accounts because there was no one else but RCBC and its personnel who had any ability to take any action with respect to the Fictitious Accounts. Moreover, the entire purpose of anti-money laundering laws and bank secrecy laws would be thwarted if fictitious accounts like those at issue here could be used as the instruments of fraud and then bank secrecy utilized as a shield in defense of that fraud.

207. Finally, as discussed in more detail below, at around 3:31 p.m. after all the fictitious accounts had been almost completely drained, RCBC senior management finally placed a hold on the Fictitious Accounts. RCBC then sent a SWIFT message to the Bank: "WE ACKNOWLEDGE RECEIPT OF YOUR NOTICE. ACTING ON YOUR INSTRUCTIONS, WE HAVE PLACED ON HOLD THE REMAINING PROCEEDS FROM THE TRANSACTIONS WHICH IS WITHOUT PREJUDICE TO ADDITIONAL INFORMATION NOTICES OR INSTRUCTIONS THAT MAY BE RECEIVED BY THE BANK, AND WHICH MAY BE CONTRARY TO YOUR INSTRUCTIONS. THANK YOU. RCBC HEAD OFFICE."

F. When Telling the Bank That It Had Finally Placed a Hold on the Fictitious Accounts, RCBC Hid from the Bank That Those Accounts Had Already Been Looted and Moved to Other RCBC Accounts and That the Laundering Was Continuing within RCBC

208. RCBC's response to the Bank's SWIFT message withheld the fact that the Fictitious Accounts had been drained almost completely but that the stolen funds still remained at RCBC in other accounts. If RCBC had informed the Bank of these facts, the Bank could have taken additional actions, including demanding RCBC to freeze the other accounts. Instead, RCBC withheld this information from the Bank. Indeed, during this whole time, the thieves continued to launder the stolen money, including engaging in foreign exchange transactions with RCBC that netted RCBC yet more substantial fees.

209. Michael Bautista—with the assistance of RCBC's own Forex Brokers Corporation, a division of RCBC able, along with RCBC's Treasury, to make foreign exchange transactions—began converting stolen funds received from the Fictitious Accounts and held in dollars in Philrem's RCBC account into Philippine pesos. On information and belief, RCBC earned substantial fees and commissions on transactions that were valued in the millions of dollars.

210. In particular, at 10:25 a.m. on February 9, on behalf of Philrem, Michael Bautista called RCBC's Forex Broker and requested the conversion rate to sell $15,000,000. The Trader at RCBC's Forex Broker offered a reduced rate of 47.74 Philippine pesos, and Michael Bautista then sold $15,000,000 from the Philrem account at RCBC's Unimart branch.

211. With essentially all of the stolen funds emptied from the Fictitious Accounts, Cuaresma checked their balances around 11:00 a.m. and discovered that they had minimal amounts remaining. Cuaresma called RCBC's Jupiter Branch to discuss the Fictitious Accounts. She spoke to Torres, who told her to talk to Deguito, who was allegedly out of the office on a client call.

212. Later that morning, Philrem continued to convert the stolen funds to pesos. At 11:40 a.m., Michael Bautista called RCBC's Forex Broker again requesting the best conversion rate for the sale of $17,000,000. Of course, by this time, RCBC had full knowledge that the stolen funds had been transferred into the Go-Centurytex Account and Philrem accounts. The fact that RCBC continued to do nothing when it could have clawed back these funds is evidence of RCBC's culpability in the theft. RCBC's Forex Broker sold $17,000,000 of the stolen funds still remaining in the Philrem account.

213. As a result of these two conversions executed by RCBC's own Forex Broker, Philrem's dollar account was debited $17,000,000 and $15,000,000 and its peso account RCBC's Unimart branch was credited 811,410,000 pesos and 716,100,000 pesos at 12:46 p.m. and 2:47 p.m., respectively. Accordingly, the stolen funds remained in an account at RCBC but now in the form of Philippine pesos. RCBC was happy to continue acting purely in its own business interest, earning substantial fees on those accounts and substantially greater fees on the foreign exchange trades, regardless of the Bank's rights and the knowledge of the nature of the stolen funds.

214. Then Deguito and Torres began moving the stolen funds themselves. At 12:40 p.m., they withdrew $13,000,000 from the Go-Centurytex Account and deposited it into an account for an entity called the Abba Currency Exchange ("**Abba Account**") at RCBC. Fifteen minutes later, they withdrew $20,000,000 from the Go-Centurytex Account and deposited it into Philrem's U.S. dollar account at RCBC.

215. At 1:00 p.m., after all of this had already happened, RCBC Compliance Officer, Maria Fe V. Salamatin, and RCBC Anti-Money Laundering ("**AML**") Head, Attorney Laurinda Rogero, received calls from Remedios Maranan, the National Service Head of the Retail Banking Group, about the SWIFT messages. Two hours later, at 3:00 p.m., the Retail Banking Group and RCBC's Legal and Regulatory Affairs Group ("**LRAG**") (which includes RCBC's Compliance and AML Groups) met to discuss the Bank's request for the recall of the remittances and to draft a reply to the SWIFT messages. At this point, the outstanding balances in the Fictitious Accounts had been drained to a mere $68,335.63.

216. The officers present at the meeting (which included Capiña and Raul Tan) agreed—after the Fictitious Account had essentially been looted—to pointlessly put a hold on those Fictitious Accounts. RCBC's Jupiter Branch enforced this hold at around 3:31 p.m., hours after the funds had been sent to other RCBC accounts held by Go and Philrem and even longer since RCBC saw the Bank's stop payment and hold requests.

217. More importantly, the same RCBC officials refused to freeze the stolen funds that were now in the Go-Centurytex Account, the Philrem dollar and peso accounts and the Abba Account, even though the thieves had already begun laundering the stolen funds to complete the theft. The RCBC officers had available to them information that showed that these other accounts held stolen funds transferred from the Fictitious Accounts but chose not to protect those stolen

funds from continued looting, and instead to pursue their business interests to collect fees on the accounts, transfers and foreign exchange trades.

218. While RCBC's senior officers were meeting and doing nothing to stop the laundering, the fraudulent transactions continued. At 3:12 p.m., $3,000,000 was transferred from the Abba Account to an account for Beacon Currency Exchange ("**Beacon Account**") also at RCBC.

219. At around 4:00 p.m., Salamatin and Rogero informed the LRAG Head, Attorney Celia Fernandez-Estavillo, about the transactions involving the Fictitious Accounts at RCBC's Jupiter branch. Estavillo then called RCBC's Internal Audit Group ("**IAG**") and asked them to investigate and conduct an audit of RCBC's Jupiter branch.

220. Finally, during the evening of February 9, 2016, RCBC sent the reply to the Bank's SWIFT messages stating that the accounts had been frozen. As discussed, these messages, sent on behalf of "RCBC HEAD OFFICE," failed to disclose that those particular accounts had already been looted and that much of the stolen funds had been funneled to other accounts held at RCBC. In other words, RCBC's Head Office made clear that it had the authority to place a hold on the Fictitious Accounts, but had not previously done so.

221. The next day, February 10, 2016, the Bank sent yet another stop payment request with respect to the Fictitious Cruz Account, with the phrase "STOPPAY" in the reference and containing the following narrative:

> TOP URGENT……..TOP URGENT……..TOP URGENT
> .
> .
> REF TO MT103 THE TRANSACTION VALUE DATE: 160204, AMOUNT: USD 6,000,039.12, ORIGINATOR IDENTIFIER: [ACCOUNT NO.], BENEFICIARY NAME: MICHAEL F. CRUZ, A/C NO OF THE BENEFICIARY: [].
> .

> PLEASE BE INFORMED THAT THIS IS A FRAUDULENT TRANSACTION AND UNAUTHORIZED ACCESS IN OUR SWIFT SYSTEM. SO YOU ARE REQUESTED TO STOP THE PAYMENT AND IF YOU HAVE ALREADY MADE THE PAYMENT THEN FREEZE THE ACCOUNT OF BENEFICIARY AND PLEASE BACK THE FUNDS TO THE ACCOUNT NO. [] WITH [THE INTERMEDIARY BANK].
> .
> [THE INTERMEDIARY BANK] HAS INFORMED US THAT THEY HAVE ALREADY SENT A FEDWIRE MESSAGE TO THE RECEIVING BANK TO CALL BACK THE FUND.
> .
> PLEASE FEEL FREE TO CONTACT US FOR FURTHER QUERY.
> .
> YOUR COOPERATION IN THIS REGARD WILL BE HIGHLY APPRECIATED.

222. That afternoon, around 1:30 p.m., Salamatin and Rogero informed Torres that suspicious transaction reports only then submitted by RCBC's Jupiter branch on the Fictitious Accounts were insufficient and that she must provide details in the AML system, demonstrating that such a system existed and was ignored or purposefully circumvented by senior RCBC personnel, requesting that she add information that the transactions were not commensurate to the clients' sources of funds. Having received no response, Salamatin and Rogero sent Torres another email at 6:06 p.m. asking for the reports the next day. Despite Torres' non-responsiveness and despite her involvement in the suspicious transactions, along with Deguito and Agarrado, the representatives from the Compliance and AML Departments did nothing—in particular, they did not go to RCBC's Jupiter branch themselves.

223. Meanwhile, during the same afternoon, RCBC's Treasury Department, through its head, Raul Tan, continued to assist Philrem convert the stolen funds from dollars to pesos. At 3:52 p.m., Michael Bautista asked the RCBC Treasury to trade $15,000,000 from the Philrem dollar account for pesos, and the Treasury executed that trade yet again, earning RCBC significant fees.

224. Raul Tan allowed Philrem's trades with the Treasury Department to proceed despite his knowledge of the suspicious nature of the funds and the Bank's request to recall them. On February 9, 2016, four days after Raul Tan first became aware of the suspicious activity in the Fictitious Accounts, he was informed by a Steven Reyes, a member of Treasury Department, about a trade with Philrem. Raul Tan instructed Reyes to ask his permission before trading with Philrem again. On February 10, 2016, Reyes advised him that Philrem wanted to trade again and Raul Tan permitted him to do so.

225. On February 10, 2016, Michael Bautista of Philrem sent Defendant Reyes a message asking about Philrem's transactions at RCBC's Unimart branch in connection with converting funds from dollars to pesos. At 11:38 a.m. that same day, Reyes forwarded a message to Bautista from RCBS Unimart's branch manager confirming that the transactions were successful. This incident occurred five days after Reyes became aware of the suspicious nature of the funds and one day after he was informed of BB's recall request.

226. At this point, instead of refusing transactions with Philrem, Reyes and Raul Tan, as they later claimed, decided to quote a very "off-market price" with the thought that "Philrem will not deal with an off-market price because Philrem was very price-sensitive and the market was about to close." Desperate to launder the money, however, Philrem made the transaction (and RCBC made better than market rates for the foreign exchange, demonstrating that RCBC would do anything to generate profits for itself at the Bank's expense). In other words, both Philrem and RCBC profited off the arrangement — Philrem got funds laundered and RCBC got additional profits (and plausible deniability based on their attempts to use such facts to demonstrate their alleged innocence).

227. The next day, February 11, despite RCBC's senior officers' knowledge of the suspicious nature of the transactions, they allowed those transactions to continue. At 3:12 p.m., $3,000,000 was transferred from the Beacon Account to Philrem's dollar account. At 3:14 p.m., $10,000,000 was transferred from the Abba Account to Philrem's dollar account. Both the Abba Account and Beacon Account had received these stolen funds from the Fictitious Accounts through other internal RCBC Accounts, including the Go-Centurytex Account. On information and belief, either Philrem or one or more of the other conspirators controlled or otherwise had access to the Beacon and Abba Accounts (for which details, including their opening dates and alleged beneficiaries, remain concealed).

228. This represented the final deposit of the money from the Fictitious Accounts into Philrem's dollar account. Of the total $81,001,617.12 deposited into the Fictitious Accounts, $80,880,000 eventually made its way to Philrem's dollar account.

229. On information and belief, RCBC made hundreds of thousands to millions of dollars on the foreign exchange transactions and other banking fees in the furtherance of this conspiracy and its own interests. RCBC has been notably silent in admitting precisely how much it profited from these transactions, which amounts will be discovered in this action.

230. After all of this was done, at 6:35 p.m., Deguito finally replied to Salamatin and Rogero's email with a suspicious transactions report. At 8:34 p.m., despite the suspicious activity and transfers occurring throughout RCBC's banking system, the AML Department simply approved those reports. Of course, by that time, the Fictitious Accounts had been already been looted.

231. Finally, on February 12, 2016, at 9:16 a.m., after all the stolen funds had been transferred out of the Go-Centurytex Account, RCBC finally filed the suspicious transaction

reports regarding the transfers in a variety of accounts including the four Fictitious Accounts, the Go-Centurytex Account, and Philrem's accounts, which are summarized as follows:

Account Holder	Transaction	Date	Amount (USD)	Remarks
Enrico Teodoro Vasquez	Inward Remittance	2/5/2016	$ 25,001,573.88	Amount involved not commensurate with the business or financial capacity of client
Jessie Christopher Magno Lagrosas	Inward Remittance	2/5/2016	$ 30,000,028.79	
Michael Francisco Cruz	Inward Remittance	2/5/2016	$ 6,000,029.12	
Alfred Vergara	Inward Remittance	2/5/2016	$ 19,999,990.00	
William So Go	Deposit - Cash	2/5/2016	$ 22,735,000.00	No underlying legal or trade obligation, purpose, or economic justification
William So Go	Deposit - Cash	2/9/2016	$ 14,323,269.46	
William So Go	Deposit - Cash	2/9/2016	$ 14,298,209.37	
William So Go	Deposit - Cash	2/9/2016	$ 14,312,185.54	
Philrem Service Corporation	Inter-Account Transfer	2/5/2016	$ 500,000.00	Deviation from client's profile/past transactions
Philrem Service Corporation	Inter-Account Transfer	2/5/2016	$ 14,200,000.00	
Philrem Service Corporation	Deposit - Cash	2/9/2016	$ 15,215,977.26	
Philrem Service Corporation	Deposit - Cash	2/9/2016	$ 20,000,000.00	

VI. THE CONSPIRATORS TRANSFER THE STOLEN FUNDS OUT OF RCBC AND FURTHER LAUNDER THEM THROUGH THE CASINOS

232. After the conspirators converted virtually all of the stolen funds ($80,691,772 of the $81,001,662.12) to Philippine pesos and transferred them to Philrem's peso account at RCBC's Unimart Branch, Philrem turned around and transferred the funds, in pesos, to accounts at other banks, from which they were then distributed to and laundered through casinos, individuals, and questionable businesses.

A. Laundering the Stolen Funds through and to Bloomberry and the Solaire Casino and Benefitting Defendants Ding, Xu, and Others

233. One of the businesses through which the conspirators laundered the stolen funds, once converted to pesos, was Bloomberry Resorts and Hotels, Inc. ("**Bloomberry**"), which owns the license for and operates the Solaire Casino. Once in the hands of the Solaire Casino, the stolen funds were then converted to three different types of casino chips and given to Defendants Ding, a Chinese national, and Xu and their associates, who used the chips at the Solaire Casino for over a month.

234. Specifically, from February 5-11, 2016, Philrem transferred approximately $2.9 billion pesos from its peso account at RCBC's Unimart branch to Eastern Hawaii Leisure, the Go-Centurytex Account, and to Philrem accounts at RCBC and three other banks: BDO, Metrobank, and Security Bank and Trust Company ("**Security Bank**").

235. Philrem then transferred 1,365,000,000 pesos from its own BDO bank account to another BDO bank account held for the benefit of Bloomberry. On February 5, 2016, Philrem made four transfers totaling 565,000,000 pesos (*Id.*):

Table 18

Date	Amount (Php)
5-Feb-16	100,000,000.00
	130,000,000.00
	200,000,000.00
	135,000,000.00
Total	**565,000,000.00**

On February 10, 2016, Philrem made another five transfers to the Bloomberry account totaling another 800,000,000 pesos:

Table 19

Date	Amount (Php)
10-Feb-16	210,000,000.00
	190,000,000.00
	200,000,000.00
	100,000,000.00
	100,000,000.00
Total	**800,000,000.00**

In total, Philrem transferred 1,365,000,000 pesos to Bloomberry's account.

236. Bloomberry, the license holder and operator of the Solaire Casino, then used all 1,365,000,000 pesos, which was approximately $29,000,000 U.S., to buy non-negotiable Solaire Casino chips for Ding, who is a Chinese national, Gao, and 17 others playing with him.

237. Defendant Ding ran casino junkets, including the "Sun City" junket, "Gold Moon" junket, and "Lau Ka Wai" junket—that is, highly profitable VIP business in casinos such as Solaire Casino, sometimes with their own dedicated playing rooms at casinos or chips that are unique to that junket—that the thieves used to launder the stolen funds. Solaire Casino also received approximately $29 million into accounts at the casino that had been withdrawn from the fictitious RCBC accounts and could be laundered through the purchase of non-negotiable casino chips.

238. As another step in laundering the funds, Ding and his associates exchanged (i) Solaire Casino chips worth 903,730,000 pesos for an equal amount of non-negotiable Sun City junket chips; (ii) Solaire Casino chips worth 100,000,000 pesos for an equal amount of non-negotiable Gold Moon junket chips; and (iii) Solaire Casino chips worth 30,195,000 pesos for an equal amount of non-negotiable Lau Ka Wai junket chips.

239. Ding and his associates played these junket chips and the remaining balance of Solaire Casino chips in Solaire Casino's Premium Program over multiple gaming sessions for over a month, from February 5 to March 10, 2016.

240. Then, on March 10, 2016, Solaire Casino ended all gaming sessions using the Solaire Casino chips traceable to the original 1,365,000,000 pesos. Solaire Casino confiscated 107,250,602 pesos worth of Solaire Casino chips (including all of the remaining junket chips) from Ding's and his associates' Solaire Casino accounts, along with cash totaling to 1,347,069 pesos.

241. It remains unclear, as Solaire has steadfastly refused to assist, precisely how and to where the money was laundered, as well as the timing of such actions. On information and belief, both the Solaire Casino and the individual Defendants profited to the tune of millions of dollars in connection with the laundering scheme. The Solaire Casino then waited until there was barely anything left before it acted.

B. Laundering the Funds through and to Eastern Hawaii Leisure and Defendant Wong

242. Another business through which the conspirators laundered the stolen funds was Eastern Hawaii Leisure. Philrem made two large transfers from its peso account at RCBC's Unimart branch to Eastern Hawaii Leisure's account at the Philippine National Bank ("**PNB**"). Although Defendant Gao was also a co-investor in Eastern Hawaii Leisure, Defendant Wong was the sole signatory on Eastern Hawaii Leisure's PNB account. Defendant Wong also had a personal account at PNB, which was also used as part of laundering the funds. By the end of February, through a series of multiple withdrawals approximately 1,000,000,000 pesos (over $20,000,000) of the stolen funds were laundered through and withdrawn from the Eastern Hawaii Leisure account.

243. Wong was ready for these funds to arrive since February 5, 2016, and likely earlier. Deguito testified that Wong had called her on February 4, 2016 to ask her to meet him at Solaire for what was obviously pretextual purposes — to discuss an issue that had arisen at Deguito's former bank at which she had not worked for nearly three years — and then, on February 5, 2016,

Wong called her at RCBC between 11:30 a.m. and 12:00 p.m. asking her to check whether a large deposit had been made in the fictitious Cruz account. There had, in the amount of approximately $6 million. Wong also called Deguito several times thereafter to discuss the accounts and the use of Philrem as a remittance company.

244. Five days later, Philrem's first transfer to Eastern Hawaii Leisure's bank account was made on February 10, 2016 in an amount just short of 500 million pesos—499,999,748.50 pesos, to be exact. That same day, Eastern Hawaii Leisure, whose sole signatory was Defendant Wong, made two withdrawals totaling 500 million pesos—one withdrawal of 400 million and the other of 100 million.

245. Wong then used his personal account to complicate the trail of these stolen funds. In particular, still on that same day, February 10, 2016, he deposited into his personal account the 400 million pesos that he had just withdrawn from the Eastern Hawaii Leisure account. Wong kept the 100 million pesos that he had withdrawn. Then, he turned around and withdrew the 400 million pesos right back out of his personal account as cash.

246. Then, the next day, February 11, 2016, he re-deposited those 400 million pesos back into the Eastern Hawaii Leisure account. These transfers were intended to create a confusing money trail and help launder the money.

247. Also on February 11, 2016, Philrem again transferred another approximately 500 million pesos into the Eastern Hawaii Leisure account—precisely, yet again, 499,999,748.50 pesos. With these two transfers of equal amounts on February 10, 2016 and February 11, 2016, Philrem had transferred from its peso account at RCBC's Unimart branch approximately $21,052,631.58 of the stolen funds.

248. From February 11 to 26, 2016, Eastern Hawaii Leisure, through Defendant Wong, executed seven withdrawals totaling just over 900 million pesos. With those withdrawals, along with the 100 million pesos withdrawn on February 10, 2016 and never redeposited, Defendant Wong and the conspirators had taken and laundered at least $21,000,000 of the stolen funds.

249. However, as discussed more fully below, Wong and other conspirators, including Philrem and the Bautistas, have offered inconsistent, misleading, and/or outright false testimony on where all of the cash and deposits went, and, as such, Wong could have received an additional approximately $14 million in stolen funds, taking Wong's total haul to $35 million (of which he returned only $15 million).

C. Laundering the Funds through Cash Deliveries by Philrem to Defendants Xu and Wong at the Solaire Casino

250. The stolen funds were also distributed and laundered through deliveries of cash on at least six occasions by Philrem to Defendant Xu, and likely Defendant Wong given the significant inconsistencies in the testimony of multiple defendants.

251. In particular, as shown in the table below, from February 5 to 13, 2016, Defendant Xu, and likely Defendant Wong, received from Philrem at the Solaire Casino deliveries totaling 600 million pesos and $18 million. Solely in dollars, these cash hand-offs totaled $30,639,141.63.

Table 25

	Received by	Date	Amount	
			Php	USD
1	Weikang Xu	2/5/16	90,000,000.00	
2	Weikang Xu	2/5/16		500,000.00
3	Weikang Xu	2/9/16	110,000,000.00	
4	Weikang Xu	2/9/16		3,000,000.00
5	Weikang Xu	2/10/16	100,000,000.00	
6	Weikang Xu	2/10/16		3,000,000.00
7	Weikang Xu	2/11/16	100,000,000.00	
8	Weikang Xu	2/11/16		2,000,000.00
9	Weikang Xu	2/12/16	100,000,000.00	
10	Weikang Xu	2/12/16		3,500,000.00
11	Weikang Xu	2/13/16	100,000,000.00	
12	Weikang Xu	2/13/16		6,000,000.00
Total			**600,000,000.00**	**18,000,000.00**

252. These cash deliveries from Philrem to Xu of $30,639,141.63 came from the $81,001,662.12 stolen from the Bank's account at the New York Fed.

VII. THE DEFENDANTS HAVE REFUSED TO PROVIDE INFORMATION OR TELL INCONSISTENT AND FALSE STORIES TO HIDE THEIR WRONGDOING AND THE MONEY THAT THEY STOLE FROM THE BANK

253. The conspirators know what they did with the Bank's stolen funds and how they were transferred through fictitious and illegitimate accounts, turned into cash, laundered through casinos and questionable businesses, and disbursed to the thieves. Yet they have refused to assist the Bank, talk to authorities and/or have given false, inconsistent testimony.

A. RCBC Is Not Talking

254. RCBC officials have claimed that bank secrecy rules prohibit them from answering questions from government regulators and the Philippines Senate's Blue Ribbon Committee as to their procedures and whether they followed them in connection with the theft.

255. RCBC was perfectly willing, however, to disclose the details of the Fictitious Accounts and the William So Go and Centurytex Trading accounts, and it was willing to describe how it claims to have cleaned up its act after the theft.

256. But when it came to explaining why RCBC allowed the stolen funds in the Fictitious Accounts to be transferred through many other RCBC accounts after stop payments had been received or identifying the ultimate recipients of the funds, RCBC would not testify.

257. For example, RCBC's Head of the Legal and Regulatory Affairs Group, Ms. Fernandez-Estavillo, would not tell the Blue Ribbon Committee whether RCBC knew of the mere fact that it had received the stolen funds on February 5, 2016:

> SEN. ENRILE. When the money in question arrived in your bank on February 5, did you know about it?
>
> MS. FERNANDEZ-ESTAVILLO. Your Honor, with all due respect, we cannot speak on that as we are covered by bank secrecy.

258. RCBC's Head of the Legal and Regulatory Affairs Group also refused to tell the Blue Ribbon Committee whether RCBC's Settlement Department followed the required procedures to review remittances that breached a certain threshold, as the unauthorized transfers did, and make a follow-up phone call to the branch that received the remittances:

> SEN. AQUINO. To your knowledge, Attorney, since you are speaking for RCBC, was a phone call made from the settlements division to Branch Manager Deguito?
>
> MS. FERNANDEZ-ESTAVILLO. You know, Your Honor, well, I would like to answer, but I cannot because we cannot speak of the specific accounts covered by bank secrecy.

259. Yet RCBC had already admitted that the "specific accounts" mentioned by RCBC's Head of Legal and Regulatory Affairs were fictitious. There can be no reasonable basis not to answer regarding a phone-call procedure for make-believe accounts. Separately, Defendant

Deguito nonetheless provided the answer in her testimony, testifying that no one at RCBC made the required phone call.

260. RCBC's President, Lorenzo Tan similarly hid behind the bank secrecy when asked why RCBC did not honor the stop payment and freeze requests sent by RCBC:

> THE CHAIRMAN. … Could you care to explain why the stop payment request, which should have been honored at the very start of the banking day, was not honored?
>
> MR. L. TAN. I am sorry, Your Honor, I cannot confirm or deny this request specific to this transaction. But as a general rule, when there is a freeze order on an account, the branch manager involved should comply with such order.
>
> THE CHAIRMAN. Did you send it to your branch manager?
>
> MR. L. TAN. Again, Your Honor, I am precluded because of bank secrecy.

261. RCBC's Head of the Legal and Regulatory Affairs Group also used the bank secrecy laws to dodge questions on whether RCBC properly followed its stop payment procedures:

> SEN. RECTO. Okay was [the stop payment] procedure followed?
>
> MS. ESTAVILLO. Your Honor, we apologize. But because of the numerous secrecy laws that are in place, we are unable to answer. . . .
>
> SEN. RECTO. Okay. And what you say [is] that you cannot inform the Committee if the procedure was followed?
>
> MS. ESTAVILLO. We cannot, Your Honor.

262. The recitation of bank secrecy rules in the face of admittedly fictitious accounts begs the question of whose secrecy RCBC even would be protecting. These were not real people at all, which RCBC had already admitted, and leads only to the conclusion that RCBC has purposefully and intentionally attempted to hide its role in the theft and money laundering.

263. RCBC has steadfastly attempted to keep the details of its involvement in the robbery as quiet as possible so that it may avoid liability. But, as the history alleged in this

Complaint shows, RCBC and its senior officials and branch management were involved months before the theft actually occurred, all the way through to the distribution of the stolen funds to the other conspirators to be laundered.

264. RCBC's conduct was so egregious that, in 2016, the Monetary Board of the Central Bank of the Philippines—Bangko Sentral ng Pilipinas—approved a 1 billion peso fine (approximately $20 million) against RCBC, the largest fine ever approved by the Central Bank of the Philippines. Although, RCBC paid that fine in two installments in late 2016 and 2017, the Bank has never seen a cent of that money.

B. Philrem, the Bautistas and Wong Gave Inconsistent Testimony on Deliveries of over $30 Million in Cash to Xu, Wong, and Others

265. Philrem and its principals, Michael and Salud Bautista, delivered 600,000,000 pesos and $18,000,000 to defendants Xu, Wong, and/or others at the Solaire Casino. Yet, before the Senate's Blue Ribbon Committee, the Bautistas and other conspirators could not get their stories straight on the foreign exchanges, cash withdrawals and handmade cash deliveries in which Philrem, Xu, Wong, and/or other conspirators participated. This testimony was a mixture of cover-up and finger-pointing that made clear that everyone was involved and must be held liable and that none of them are telling the whole truth.

266. Philrem's involvement, from the start, was intended, among other things, to create a confusing money trail. According to the Philippine Department of Justice, Philrem "was to make it extremely difficult to trace the source and flow of the funds." Philrem "commingled the funds and acted as a 'clearing house.'"

267. Along those lines, the Bautistas made six cash deliveries of funds from the Philrem peso account to Defendant Xu and Wong. The Blue Ribbon Committee Report identified numerous discrepancies in Defendants' testimony about these handoffs.

268. The first cash delivery, on February 5, 2016, was of 90 million pesos and $500,000. Salud Bautista testified to the Blue Ribbon Committee that she supposedly made this first delivery to Xu at the Solaire Casino. Purported receipts for that delivery, however, indicate that Mark Palmares, a Philrem messenger, delivered the funds directly to Xu. Yet that is contradicted by Mr. Palmares' testimony that he only delivered the funds to Salud Bautista, who supposedly delivered them to Xu (although Mr. Palmares did not see Xu). Defendant Kim Wong had yet a different story. He testified that he received the delivery, not Xu, that it was only 100 million pesos, and that Michael Bautista and Deguito made the delivery.

269. The second cash delivery, on February 9, 2016, was of 110 million pesos and $3 million. Michael Bautista testified that he made this delivery at his own home to both Xu and Wong. Mark Palmares testified that he delivered the funds to Michael Bautista but never saw Xu. Wong testified that he arrived at the Bautistas home alone, without Xu, and picked up the cash.

270. The third cash delivery, on February 10, 2016, was of 100 million pesos and $3 million. Michael Bautista testified that he made this delivery to Xu at Bautista's home. Philrem's receipts, however indicate that Mark Palmares delivered the cash to Xu. Palmares disputes this, claiming that he gave the cash to Michael Bautista. Kim Wong, on the other hand, testified that he received the delivery and that he received only $2 million (not $3 million) along with the 100 million pesos.

271. The fourth cash delivery, on February 11, 2016, was of 100 million pesos and $2 million. Michael Bautista testified that he delivered this cash to Wong and Xu. Philrem's receipts, however, show that Palmares delivered it to only Xu. And Palmares testified that he delivered the cash only to Michael Bautista and never even saw Xu. Kim Wong denied ever being there on February 11.

272. The fifth and sixth cash deliveries, on February 12 and 13, were, respectively, of 100 million pesos and $3.5 million, and 100 million pesos and $6 million. Michael Bautista testified that Xu picked up the cash and that Wong was not there. The Philrem receipts, however, show that Palmares delivered the cash to Xu. But Palmares testified that he left the cash with Michael Bautista and never saw Xu. Kim Wong at that point claimed that Xu never went to the Bautista's home to pick up cash.

273. Salud Bautista has a different story from everyone else. In her March 15, 2016 testimony, she said that all $18 million were delivered to Xu at the Solaire Casino. She also testified that she met Wong only once or twice and that it was years earlier. Despite that, she also testified that Wong was present at all cash deliveries with Xu. Two weeks later, on March 29, 2016, she testified that at least one of the deliveries occurred at the Bautistas home and that only Wong was there.

274. The Bautistas also gave false testimony on the huge amount of fees that they made on these transactions/deliveries. At first, Salud Bautista testified that Philrem only made 500 pesos in fees (approximately $9.48). Later, under further questioning, she admitted that Philrem earned more than 10,450,000 million pesos (approximately $200,000).

275. This finger-pointing and false testimony among thieves resulted in wildly different stories on the amounts of the stolen funds laundered in this way. The Bautistas claimed that they delivered 600 million pesos and $18 million in cash. Wong testified that Philrem delivered only 400 million pesos and $5 million. Converted to dollars, this is a discrepancy of approximately $17.2 million.

276. Moreover, none of this appeared in the suspicious transaction report filed by Philrem on February 17, 2016, on information and belief, to provide them plausible deniability

after the fact and hide their culpability. The STR glaringly omitted that Wong directly received any funds.

277. What is clear, though, is that the Bautistas, Wong, Xu, Philrem, and the others were involved, are culpable, and should be held liable for stealing from the Bank.

C. Eastern Hawaii Leisure, Wong, Gao, and Ding Were Involved in the Theft but Their Laundering and Storytelling Make the Money Trail Hard to Follow

278. In addition to his involvement with Philrem and Xu, Wong has refused to explain discrepancies and highly suspicious transfers related to Eastern Hawaii Leisure and Wong.

279. For example, as alleged earlier, Philrem transferred one billion pesos to Eastern Hawaii Leisure and Wong. From that, 550 million pesos were transferred to a junket in Midas Casino run by Wong, and those chips were played at that junket in the Midas Casino. Eastern Hawaii Leisure and Wong — by and through the participants in his junket — played those chips until March 2, 2016. By then, only 40 million pesos worth of chips remained. The remainder of the chips were gone, cashed in for untraceable cash after being played by the participants in Wong's junket. It is unclear who has this money and precisely how much remained after they were laundered through this gambling process.

280. Additionally, of the at least 400 million pesos and $5 million in cash supposedly provided to Wong (by his claim) by Philrem, he brought 100 million pesos to a junket at the Solaire Casino on February 5, 2016. He deposited the remaining 300 million pesos in another casino junket, on information and belief the junket he was running at the Midas Casino, but it is unclear whether these funds were ever converted into chips and played. Wong deposited the $5 million U.S. at the Solaire Casino for one of the junkets. Gao and Ding then took $370,000 of these funds in cash, but it is unclear if they ever converted those funds to chips and then played them.

281. Wong and Eastern Hawaii Leisure did not stop the play at Midas Casino until March 2, 2016, after an unknown amount of the funds had been played and laundered.

282. Finally, Defendants Ding and Gao, are well known as individuals who have run (and, in Gao's case, been convicted of running) illegal gambling operations and foreign gaming junkets for years. Notably, they were familiar with Macau, a location in which North Korean persons, such as hackers, are reported to maintain covert bank accounts. *See* Baccarat Binge.

D. There Is No Real Dispute That These Stolen Funds Were Laundered by Wong, Eastern Hawaii Leisure, and the Other Defendants

283. There can be no serious claim that the funds were not being laundered through RCBC and the casinos. Indeed, court filings in the Philippines in connection with the surrender by Defendants Wong and Eastern Hawaii Leisure have laid bare the scheme even if its details may remain hidden by the trail of lies and misrepresentations offered by Defendants.

284. Despite that they accepted at least $21 million, Defendants Eastern Hawaii Leisure and Kim Wong returned only $15 million of those funds, calling into question where the remaining at least $6 million or more is located.

285. The return also calls into question where the money went after Wong and Eastern Hawaii Leisure received it, regarding which Wong has been tight-lipped. Instead, Wong, on behalf of himself and Eastern Hawaii Leisure, sent his lawyers to the AMLC with bags of Pesos and U.S. dollars, together worth the $15 million he was returning, with no explanation for where it had been before being dropped off at AMLC.

286. In connection with forfeiture proceedings in connection with those funds, during which the Makati Regional Trial Court of the Philippines was to determine whether to return the funds to the Bank, the Philippines government itself admitted that the funds "are part of the foreign reserve money of the Bangladesh Bank (BB), stolen by cyber thieves or hackers from its account

maintained with the Federal Reserve Bank of New York." As such, the court granted the return of the funds, stating that it had "been established" that the account of the Bank had been hacked and the money routed through RCBC accounts.

287. Indeed, the only thing Wong has admitted — to the Blue Ribbon Committee — is that he took 450 million pesos from the funds as payment for an antecedent debt that Defendant Gao allegedly owed him. In other words, Wong himself, despite admitting that the funds were stolen from the Bank and that he was aware of that fact, still took some of those funds for his own personal use and business dealings with another one of the co-conspirators that was involved in the laundering of the theft of the funds.

E. Solaire Casino Has Never Come Clean on Its Central Role in Laundering the Funds

288. Solaire Casino was no better and has consistently refused to explain where the money went and why it took them so long to halt play with chips purchased with the stolen funds.

289. As a general matter, money laundering through a casino involves the deposit of cash into accounts at the casino, like Solaire, which players can convert to chips, including specialty chips unique to a junket. Then, the money launderers play those chips, typically betting on both the house's hand and the players' hands to strike a balance between gains and losses. The point is not necessarily to win more than one started with but to hide the fact that the intention is purely to turn in the chips at the end of the night for clean, untraceable cash.

290. For example, Philrem transferred 1,365,000,000 pesos to Bloomberry, who holds the license for and operates the Solaire Casino. The Solaire Casino then allowed Ding, Gao and eighteen other players to withdraw these stolen funds as chips to be played on their tables.

291. Solaire Casino allowed that active play with these chips until March 10, 2016, over a month after the theft from the Bank and despite no doubt knowing that the chips were purchased

with the funds stolen from the Bank. By that time, approximately $2 million remained of what had been approximately $29 million of the stolen funds. The rest was gone.

292. Then, despite the Solaire Casino's corporate secretary having identified Xu as having played at the casino at that time, Solaire Casino later wrote a March 29, 2016 letter stating that the corporate secretary was mistaken, now claiming that it was Ding and that Solaire Casino "does not know and had no dealings with Weikang Xu."

293. Given the many inconsistencies and falsehoods in the stories of the Defendants, it remains unclear whether Xu delivered these funds to Defendant Ding or another co-conspirator or both, as Solaire Casino has changed its story and now claims that its dealings were with Defendant Ding, not Xu.

294. The testimony, stories, finger-pointing and inconsistencies make one thing clear: each of these Defendants were involved in the conspiracy to steal and launder funds held in the Bank's account at the New York Fed, and each of these Defendants should be held liable.

AS AND FOR A FIRST CAUSE OF ACTION

(Conversion / Theft / Misappropriation Against All Defendants)

295. Plaintiff repeats and realleges the allegations contained in paragraphs 1 through 294 as if fully set forth below.

296. The Bank held a particular and definite sum of money, $81,001,662.12, in a bank account identified by its distinct account number at the New York Fed.

297. These funds were at all times the property of the Bank, and the Bank had the legal right to possess them.

298. Defendants individually and collectively interfered with, and exercised unlawful dominion and control over, the stolen funds in derogation to the Bank's exclusive rights to possess them.

299. No one at the Bank ever provided the hackers or any of the conspirators with authority to access or possess any of the Bank's funds or other property.

300. Indeed, Defendants engaged in the conspiracy alleged in this action with the specific intent and goal of stealing the $81,001,662.12.

301. Each of the Defendants played an integral part in the theft and laundering of this money. Multiple millions of dollars in cash were either secreted or used by the Defendants in contravention of the Bank's rights to those funds.

302. Each of the Defendants received and laundered funds at one point during the conspiracy and, on information and belief, converted, stole, and misappropriated certain of those funds, in amounts to be proved at trial, before assisting the other Defendants in laundering and converting the remaining proceeds.

303. RCBC, through its branch level personnel and senior officials acting within their scope of employment and to advance the business interests of RCBC, opened the Fictitious Accounts and the Go-Centurytex Account and allowed the stolen funds to be transferred through those and other accounts at RCBC for the purpose of laundering funds that they knew had been stolen. They allowed the removal of and affirmatively did remove the account holds that had been administratively put in place on the Fictitious Accounts for a short-period of approximately 45 minutes. Through these actions, RCBC and the other RCBC Defendants, exercised dominion and control over the stolen funds rightfully possessed by the Bank, did so knowing that the stolen funds had been unlawfully converted, and did so in derogation of the Bank's rights to possess them. As a result of these acts, RCBC earned substantial fees on the accounts through which these converted funds had been laundered and earned substantially greater fees on the foreign exchange trades that RCBC executed with these stolen funds.

304. RCBC, through its branch level managers and senior officials acting in the scope of their employment and to advance the business interests of RCBC, delayed implementing the stop payment and hold requests sent by the Bank on February 8, 2016, so as to allow nearly $60 million of the approximately $81 million in stolen funds to be routed out of the Fictitious Accounts to other RCBC accounts—after the stop payment and hold requests were received. Given that the Fictitious Accounts had no actual beneficiaries, RCBC was the only entity empowered to make those improper transfers. Through these actions, RCBC and the other RCBC Defendants, once again, exercised dominion and control over the stolen funds rightfully possessed by the Bank, did so knowing that the stolen funds had been unlawfully converted, and did so in derogation of the Bank's rights to possess them. As a result, RCBC earned substantial fees on the accounts and earned even more substantial fees on the foreign exchange trades that it executed with these stolen funds.

305. Each of the RCBC Defendants had a role, acting within the scope of their employment and empowered to take the actions that they did, from opening the accounts, to transferring the funds, to executing the foreign exchange transactions, to cash withdrawals, to the decision to release the hold, and ultimately to the abject failures to implement and enforce the stop payments sent by the Bank.

306. Defendants Raul Tan, Reyes, Capiña, and Pineda were instrumental in the decision to lift the initial hold and it was within their scope of employment to make such decisions. Defendants Deguito, Torres, and Agarrado were employees located at the Jupiter branch and were acting within their scope of employment and in the business interests of RCBC when they opened the accounts, transferred the funds, withdrew cash, and facilitated everyday banking activities that were part and parcel to the money laundering and theft scheme. Defendant Lorenzo Tan, who had

recruited Deguito to join the bank, was the nexus to Defendant Wong, who had a role in soliciting the opening of the Fictitious Accounts with RCBC personnel. Mr. Tan propped Defendant Wong up as an important person that should be "taken care of" by RCBC bank personnel as part of their scope of employment and to further the business interests of RCBC.

307. Philrem and the Bautistas converted the Bank's stolen funds into the five managers checks worth 635,000,000 pesos that listed Philrem as the payee and were deposited into Philrem's accounts at BDO and Metrobank. Philrem also received virtually the entirety of the stolen cash, after laundering and converting it through multiple unnecessary foreign exchange transactions that generated profits for Philrem, the Bautistas, RCBC. Through these actions, Philrem and the Bautistas exercised dominion and control over the stolen funds rightfully possessed by the Bank, did so knowing that the stolen funds had been unlawfully converted, and did so in derogation of the Bank's rights to possess them.

308. Defendants Centurytex and William So Go also opened and funneled funds through various accounts at RCBC in furtherance of the theft and money laundering scheme. Indeed, Centurytex and William So Go may also have received a large cash payment through the window of a Lexus parked outside the RCBC Jupiter Branch. Through these actions, Centurytex and William So Go exercised dominion and control over the stolen funds rightfully possessed by the Bank, did so knowing that the stolen funds had been unlawfully converted, and did so in derogation of the Bank's rights to possess them. Defendants Centurytex and William So Go converted and retained the stolen funds in an amount to be fully established at trial.

309. Solaire Casino received millions in cash deliveries on the grounds of its casino and placed millions more into the betting accounts at its casino, issuing special junket chips meant to enable the laundering of the funds. On information and belief, Solaire Casino retained millions of

the stolen funds and converted millions into gambling winnings for the house. Through these actions, Solaire Casino exercised dominion and control over the stolen funds rightfully possessed by the Bank, did so knowing that the stolen funds had been unlawfully converted, and did so in derogation of the Bank's rights to possess them.

310. Eastern Hawaii Leisure and Wong did the same. Defendant Wong was involved in setting up the Fictitious Accounts from the beginning of the conspiracy and received, as did his company Eastern Hawaii Leisure, millions of dollars in deliveries of the stolen cash. Eastern Hawaii Leisure and Wong accepted at least approximately $21 million (and potentially as much as $35 million). Mr. Wong returned $15 million of those stolen funds, which is an admission that he converted the Bank's stolen funds, but he has not returned the remainder of the stolen funds that he converted. Moreover, Defendant Wong testified that he accepted at least 450 million pesos of the stolen funds for the repayment of a debt to Gao, another one of the money launderers, admitting further to his conversion of the Bank's property. Through these actions, Defendants Eastern Hawaii Leisure and Wong exercised dominion and control over the stolen funds rightfully possessed by the Bank, did so knowing that the stolen funds had been unlawfully converted, and did so in derogation of the Bank's rights to possess them.

311. Finally, Defendants Xu, Ding, and Gao were all recipients of cash from the funds stolen from the Bank and/or casino chips purchased by those funds. On information and belief, these individuals, who all disappeared out of the Philippines back to China and Macau, or some other locale, shortly after they completed laundering the funds and before they could be caught, have converted and kept substantial amounts of the Bank's funds. Through these actions, Defendants Xu, Ding, and Gao exercised dominion and control over the stolen funds rightfully

possessed by the Bank, did so knowing that the stolen funds had been unlawfully converted, and did so in derogation of the Bank's rights to possess them.

312. As a result, the Bank has suffered damages in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, and other damages, that may be proved at trial.

AS AND FOR A SECOND CAUSE OF ACTION

(Aiding and Abetting Conversion / Theft / Misappropriation Against All Defendants)

313. Plaintiff repeats and realleges the allegations contained in paragraphs 1 through 312 as if fully set forth below.

314. As set forth above, the various Defendants individually and collectively converted, stole, and misappropriated funds belonging to the Bank, without authority to access or possess any of the Bank's funds, and in doing so exercised unlawful dominion and control over, the stolen funds in derogation to the Bank's exclusive rights to possess them.

315. Each of the Defendants had actual knowledge that each of the other Defendants with whom they interacted in the course of laundering and converting the funds did not own the funds or have any authority to access or possess them.

316. Yet, each of the Defendants nonetheless aided and abetted each of the other Defendants in continuing to launder and convert those funds, and accepted the benefits of the conversion, theft, and misappropriation.

317. For example, the RCBC Defendants stayed just ahead of efforts to halt the money laundering, in some cases by mere minutes. This confirms that each RCBC Defendant, acting within the scope of their employment and to further RCBS's business interests, had a role in the conversion, including the following: opening the accounts; transferring the funds; cash withdrawals; releasing the hold; failing to implement and enforce the stop payments sent by the

Bank; issuing false and misleading responses to the Bank's stop payments; and allowing laundering of the funds through accounts at RCBC, and through the RCBC Treasury, for days after the Fictitious Accounts had been frozen.

318. Likewise, Philrem and the Bautistas started making calls and setting up foreign exchanges before funds even hit the Fictitious Accounts, causing Deguito and Torres to scramble to find other outlets for the laundered funds. Philrem and the Bautistas also consistently lied and misled about the amount and destination of the funds, designed to throw the Bank and anyone hoping to stop the theft off the trail. That was the purpose of their unnecessary foreign exchange transfers and convoluted path of multi-account transfers, despite that those transfers and a money remitter like Philrem was not even necessary to the transfers if they had been legitimate and Philrem was not even licensed as a foreign exchange trader. These were all acts designed to launder the funds and aid and abet the conversion of these funds.

319. Centurytex and Go also opened accounts in July 2014 and February 2016, either alone or by and through RCBC personnel acting within their authority and scope of employment, then have given conflicting statements about those accounts, most recently claiming that the accounts were never Centurytex's or Go's despite activity in the peso account between 2014 and 2015. Defendant Go also may have received cash payments from Deguito and/or Torres, although even the testimony between the numerous parties on that is inconsistent at best. Centurytex and Go are just another part of the web of lies intended to aid and abet a successful theft of the Bank's funds.

320. Likewise Eastern Hawaii Leisure and Wong have acted as a bridge between the bank accounts and the casinos, ferrying money back and forth and were even involved in the opening of the accounts. Wong, in particular, has admitted to converting some of the funds for his

own benefit, to repay an antecedent debt to another one of the conspirators. Moreover, Wong's attempt to return certain of the funds on his own and Eastern Hawaii Leisure's behalf, but his abject failure to explain where the remaining $6 million to $20 million or more went, demonstrates their culpability. Plainly, Wong and Eastern Hawaii Leisure are another necessary part of the web of conspirators assisting and intending to assist the theft of the Bank's funds.

321. Solaire also received millions in cash to convert into chips and launder through the casino. Then, despite knowing by well before that the funds were stolen, Solaire waited until March 10, 2016 to stop the play – essentially waiting until most of the funds and chips were long gone (and despite that the other casino in this case, Midas, stopped play over a week earlier on March 2, 2016, further demonstrating Solaire's culpability). Then, after the heist, the inconsistencies continued in an effort to continue protecting the conversion of the Bank's funds. Solaire explained that in fact it had no idea who Xu was, despite that it averred previously that he had received huge amounts of money, and it only knew Defendant Ding.

322. Finally, Defendants Xu, Ding, and Gao received millions in cash and chips and laundered it through the casinos as quickly as possible before skipping town back to China and Macau, or some other locale, shortly thereafter. No other explanation follows but that these three individuals helped each of the others fulfill their part before Xu, Ding, and Gao disappeared out of the country with the Bank's funds, now fully clean and untraceable.

323. As a result, the Bank has suffered damages in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, and other damages, that may be proved at trial.

AS AND FOR A THIRD CAUSE OF ACTION
(Fraud Against RCBC)

324. Plaintiff repeats and realleges the allegations contained in paragraphs 1 through 323 as if fully set forth below.

325. As set forth above, the conspirators used fraudulent payment orders to cause the New York Fed to transfer $81,001,662.12 of the Bank's property to accounts at RCBC via intermediary banks in the United States. RCBC knowingly and intentionally facilitated the creation and use of the fictitious bank accounts at RCBC, in violation of, among other things, anti-money laundering laws, that would be used to accept and launder the funds received from the Bank's account at the New York Fed. Numerous RCBC personnel, including senior RCBC officials, knew or recklessly disregarded the fictitious nature of the accounts, including the five Fictitious Accounts and the Go-Centurytex Account, and allowed funds to be deposited therein on February 5, 2016 nonetheless.

326. On February 8, 2016, the Bank attempted to recover its funds by issuing stop payment and hold requests. Notwithstanding that RCBC delayed acting upon those requests on the next business day, February 9, 2016, when the Fictitious Accounts had been almost completely emptied looted before placing a hold on them, RCBC sent messages that RCBC had placed a hold on the Fictitious Accounts.

327. However, these statements were false and misleading, and intentionally omitting material information, including that the Fictitious Accounts were in fact fictitious and that, before RCBC put the hold in place (but after the Bank sent its stop payment and hold requests), the RCBC Defendants and the Banking-Related Defendants had almost completely emptied the Fictitious Accounts and shifted the Bank's stolen funds to other accounts still within RCBC.

328. The Bank reasonably relied on the completeness and accuracy of each of these statements and responses to the stop payment requests — in particular, the Bank relied on RCBC and that it would not omit material and important information. Had RCBC not omitted material facts that made these statements materially misleading, the Bank could and would have taken other actions to recover its funds, including requesting a hold on those other accounts to which the stolen funds had been shifted and preventing the Banking-Related Defendants from withdrawing the stolen funds from RCBC and further laundering them.

329. The RCBC Defendants did not disclose this material information that they omitted from their response to the Bank, cure their misleading statements, until well after the funds had left RCBC.

330. Consistent with all of these individuals acting within the scope of their employment and authority to provide these materially misleading statements, RCBC profited from this fraud, as it continued to reap substantial fees by holding the stolen funds in the other RCBC accounts, executed transfers of those funds between accounts, and executed highly profitable foreign exchange trades converting dollars to pesos to further facilitate the laundering of the accounts.

331. These intentional and material omissions prevented the Bank from recovering the stolen funds that remained in RCBC accounts at that time that RCBC issued the misleading response to the Bank's stop payment and hold request, and thereby damaged the Bank in an amount equal to tens of millions of dollars that the Bank could have recovered before the stolen funds had been completely withdrawn from the RCBC accounts several days later.

332. As a result, the Bank has suffered damages in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, and other damages that may be proved at trial.

AS AND FOR A FOURTH CAUSE OF ACTION
(Aiding and Abetting Fraud Against All Defendants)

333. Plaintiff repeats and realleges the allegations contained in paragraphs 1 through 332 as if fully set forth below.

334. As stated more fully above, the North Korean hackers—on behalf of and in furtherance of the conspiracy—used malicious computer malware to attack and infiltrate the Bank, duping the Bank's systems with its spear-phishing campaign and installing the malware that would fraudulently represent itself as authorized Bank personnel. In doing so, the hackers were able to create and send 70 fraudulent payment orders to the New York Fed on February 4, 2016, essentially 70 false statements that the Bank wished the New York Fed to transfer its funds to the beneficiaries selected by the North Korean hackers.

335. In fact, the Bank had no intention of allowing the North Korean hackers or any of the conspirators to access or possess any of the Bank's funds or other property, or send these false statements of its intent with respect to the funds.

336. The North Korean hackers, on the other hand, intended to deceive and hide their true activities from both the Bank and the New York Fed, which is precisely why they waited to spring into action after the close of business on a holiday weekend, after surveilling the Bank's networks for over a year and setting up the mechanisms for laundering the money through the other conspirators.

337. The Bank's systems and its agent as a repository of the Bank's funds, the New York Fed, relied upon and accepted the North Korean hackers' wrongful access to the Bank's systems and the fraudulent payment orders sent therefrom.

338. As a result of such reliance on the fraudulent payment orders, the New York Fed transferred, and the conspirators spirited away, approximately $81 million of the Bank's property.

339. The other Defendants each had their role to play in removing the funds from the United States, funneling it through accounts in the Philippines, laundering the funds out of the Philippines banking system, and to its ultimate destination, which has yet to be uncovered.

340. For example, as discussed more fully in this complaint, each of the Banking-Related Defendants, among other things, knowingly and intentionally facilitated the transfer of funds through the accounts at RCBC, conducted foreign exchange transactions, received transaction fees for their efforts, failed to make necessary reports or call into question these highly suspicious transactions, and even made cash deliveries (and potentially retained cash for themselves) in furtherance of the laundering and theft of the funds.

341. Indeed, as discussed more fully in this complaint, the RCBC Defendants, including Deguito and Torres, with the knowledge and support, or at least reckless disregard for the truth, knowingly and intentionally facilitated the creation and use of the accounts at RCBC that would be used to accept and launder the funds received from the Bank's account at the New York Fed, via intermediary banks in the United States (including in New York). Indeed, the funds were routed through numerous accounts at RCBC over a multiple day period (including when stop payment orders had been sent), generating hundreds of thousands if not millions in bank fees and foreign exchange transactions fees for transactions with the RCBC Treasury, from which RCBC profited handsomely, and employees and agents even at the highest levels of RCBC did nothing to stop the transactions or prevent the funneling of the funds through multiple accounts at RCBC and the subsequent highly suspicious cash withdrawals. Instead, RCBC's Head Office sent a misleading and materially false response to the stop payment request that would prevent the Bank from realizing that the vast majority of the funds had since moved to other accounts within RCBC. Moreover, Deguito and Torres were involved in several cash transactions that required the delivery

of cash and approval from other departments of RCBC (and were themselves involved in fraudulently papering certain transactions as cash transactions when they were in fact funds transfers), including, on information and belief, providing Deguito and/or Torres with a cardboard box with at least 20 million pesos in cash. In doing so, RCBC Defendants provided substantial assistance to advance the commission of the fraud, ensure its success, and prevent the Bank from recovering the funds.

342. As discussed more fully in this complaint, Defendants Philrem and the Bautistas knowingly and intentionally facilitated the transfer of funds through the accounts at RCBC, conducted foreign exchange transactions, received transaction fees for their efforts, failed to make necessary reports or call into question these highly suspicious transactions, stole cash out of the Go-Centurytex Account to convert into manager's (cashier's) checks which they delivered into a Philrem account at another bank, and even made cash deliveries (and potentially retained cash for themselves) in furtherance of the laundering and theft of the funds. Likewise, as discussed more fully above, these defendants also had plenty of opportunities to speak and to give accurate statements but refused. For example, despite that Philrem and the Bautistas filed a suspicious transaction report on February 17, 2016, that report was filled with errors and falsities. Through this extensive misconduct, Philrem and the Bautistas provided substantial assistance to advance the commission of the fraud, ensure its success, and prevent the Bank from recovering the funds.

343. As discussed more fully in this complaint, Defendants Centurytex and William So Go knowingly and intentionally facilitated the creation and use of the accounts at RCBC that would be used to accept and launder the funds, conduct foreign exchange transactions, and allow the other Defendants and conspirators to launder and steal the funds. The creation of the earlier peso account in the name of Go and Centurytex was just a prelude to the theft and enabled the creation of the

later account, on the day of the theft on a moment's notice with minimal documentation (and what documentation was provided was false, although Go now claims inconsistently that the peso account, which did have some transactions after its opening, was never his either). Defendants So Go and Centurytex also could have responded truthfully when asked about his role much earlier instead of waiting until as late as March 2016 to claim that he had not opened the Go-Centurytex Account that was a linchpin to the success of the laundering operation. Through this extensive misconduct, Centurytex and William So Go provided substantial assistance to advance the commission of the fraud, ensure its success, and prevent the Bank from recovering the funds.

344. As discussed more fully in this complaint, the Casino-Related Defendants, including Solaire Casino, Weikang Xu, Ding Zhize, Eastern Hawaii Leisure, Kim Wong, and Gao Shuhua, knowingly and intentionally coordinated the delivery and receipt of the funds from the other Defendants into the casinos and betting accounts (for chip purchases) that would be used to launder the funds prior to their delivery to their ultimate destination. Although Defendants Kim Wong and Eastern Hawaii Leisure returned approximately $15 million of the at least $21 million (and potentially as much as $35 million) they received, the other $6 million to $20 million remains missing. In connection with the forfeiture order for the $15 million, the Philippine courts concluded and Wong admitted that the funds were laundered, yet he has failed consistently to explain where the other money he received went (and even the amounts he received are in dispute with Wong claiming one thing, Philrem claiming another, leading to the conclusion that one or both of them must be lying).

345. With respect to Solaire Casino, Weikang Xu, Ding Zhize, and Gao Shuhua, these Defendants have returned nothing and have retained substantial profits and winnings from the gambling operations that were used to launder the funds. Despite that Solaire and the various

individuals knew or recklessly disregarded that these funds were stolen, they waited nearly three weeks to stop the gambling that was the mechanism for laundering the funds – waiting until the funds were almost completely laundered. Moreover, among other things, Solaire, which received huge amounts of cash and transfers to its casino, subsequently reversed course and told a different story about who the gambler and recipient of the funds was, yet another inconsistency proving that one or more, or all, of the participants are lying. In doing so, Solaire Casino, Weikang Xu, Ding Zhize, Eastern Hawaii Leisure, Kim Wong, and Gao Shuhua provided substantial assistance to advance the commission of the fraud, ensure its success, and prevent the Bank from recovering the funds.

346. It was not until March 2, 2016 in Midas Casino and March 10, 2016 in Solaire Casino that the Casino-Related Defendants finally stopped the play – in actuality, the money laundering – and admitted that stolen funds were being played in the casinos. By that time, the laundering was near complete, and only a small amount of the stolen funds remained.

347. Each of these Defendants failed to disclose, at every step of the way, their role and where the funds had gone and, when they did speak, omitted material facts that would have assisted the Bank in recovering its stolen funds. If they had been completely truthful and accurate, the Bank may have been able to pursue other mechanisms for recovering its funds including freezing other accounts and/or stopping the further laundering of the funds through the Casino-Related Defendants before they had all been laundered in early March 2016.

348. As a result, the Bank has suffered damages in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, and other damages, that may be proved at trial.

AS AND FOR A FIFTH CAUSE OF ACTION

(Conspiracy to Commit Conversion and Fraud against All Defendants)

349. Plaintiff repeats and realleges the allegations contained in paragraphs 1 through 348 as if fully set forth below.

350. Under New York law, consistent with the Second Restatement of Torts, civil conspiracy is a cognizable tort to the extent it alleges the existence of a conspiracy to connect the actions of the individual Defendants with an actionable, underlying tort, and establish that those actions were part of a common scheme.

351. In addition to their individual and joint and several liability for committing conversion, trespass, and fraud (and aiding and abetting each other's fraud), Defendants are also liable for the civil conspiracy to commit the foregoing causes of action one through three.

352. Upon information and belief, the Defendants all entered into an agreement to participate in a scheme to launder funds obtained through illicit means from the United States.

353. The North Korean hackers stole the funds from the Bank's account at the New York Fed, in particular approximately $81 million of the nearly $1 billion that they attempted to steal. The hackers, however, needed co-conspirators who could then remove the funds from United States, receive the funds at foreign bank in which the funds could be shifted between accounts and converted to other money as part of the laundering process, and then withdrawn from the bank and moved into untraceable channels to complete the laundering, such as casinos in the Philippines that were not, at the time, subject to Philippine anti-money laundering laws.

354. A conspiracy and agreement among the Defendants explains why fictitious dollar accounts were surreptitiously created at RCBC, through its personnel acting in their scope of employment with the authority that RCBC conveyed upon them, nearly a year before the theft, then a variety of fictitious accounts were created and used by Philrem, the Bautistas, Centurytex,

and William So Go for the purposes of, when needed, quickly transferring the funds among these accounts.

355. Likewise, Solaire Casino, Eastern Hawaii Leisure, Kim Wong, Weikang Xu, Ding Zhize, and Gao Shuhua were all ready and willing to pull massive amounts of cash out of the RCBC accounts and dump them into the murky waters of casinos and junkets and their accounts, chip purchasing operations and non-traceable gambling.

356. The operation of this historically large heist ran smoothly, with each conspirator in place to perform their assigned role, and they did so.

357. Furthermore, approximately $17 million in cash did not end up being converted into chips at the casinos despite being delivered, and it remains unknown exactly where that cash went.

358. On information and belief, one or more, or all, of Defendants obtained a portion of the Bank's stolen funds or other compensation for their participation in the conspiracy. For example, at the very least, RCBC received fees from account activity and, most profitable, foreign exchange transfers through the RCBC Treasury. Defendant Deguito generated substantial fees for her employer and transferred and removed large amounts of cash from an RCBC branch once the closed circuit television cameras had been taken offline. Likewise, Philrem and the Bautistas received potentially hundreds of thousands of dollars in fees for their work and had massive amounts of cash delivered to their home. Centurytex and William So Go had funds routed through their accounts and also may have received a large cash payment outside of the RCBC Jupiter Branch. Solaire Casino had millions of dollars routed into its casino and chip accounts, leading to millions of dollars of gambling for over one month, with Solaire profiting mightily on this gambling. Eastern Hawaii Leisure and Kim Wong received potentially tens of millions of dollars,

being forced to return some of the money, but with at least $6 million, and potentially as much as $20 million or more (depending on which of the inconsistent stories as to cash deliveries is true), still outstanding. The individuals that received funds at the casino—including Weikang Xu, Ding Zhize, and Gao Shuhua—received millions in betting chips and then disappeared from the country once it became clear that they would be implicated in the theft and laundering of the funds.

359. The Defendants knowingly and intentionally participated in the furtherance of the plan to steal and launder funds and were rewarded handsomely for that participation.

360. As a result of this conspiracy to commit these various torts, the Bank has been damaged in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, and other damages, that may be proved at trial.

AS AND FOR A SIXTH CAUSE OF ACTION

(Conspiracy to Commit Trespass Against Chattels Against All Defendants)

361. Plaintiff repeats and realleges the allegations contained in paragraphs 1 through 360 as if fully set forth below.

362. In addition to the theft of the funds, the North Korean hackers—at the direction of and in furtherance of the conspiracy—also exercised unlawful dominion and control over the Bank's property when it hacked into the computer systems of the Bank and deleted numerous key computer files in an effort to cover their tracks, in violation of the Bank's property rights.

363. At all times, the Bank owned and/or had exclusive rights to possess the computer hardware and software across its networks and its connection to the SWIFT system through which the conspirators caused the fraudulent payment orders to be sent. These networks, hardware, and software constitutes property of the Bank.

364. As early as late 2014, the North Korean hackers began to surveil the Bank's networks and made numerous surreptitious and covert attacks and attempts to infiltrate the Bank's

networks. Over the next months until they commenced their attempts to steal nearly $1 billion of the Bank's funds on February 4, 2016, the North Korean hackers gradually infiltrated the network, infecting the computers and network and placing malware on those systems. Finally, the North Korean hackers moved across the Bank's computer network into the SWIFT system, leaving malware and a trail of property destruction in their wake. Each of these movements and infection of the Bank's network and computers constituted a trespass upon the Bank's property, and provided the North Korean hackers with unauthorized access to the Bank's property in its computer systems and network.

365. No one at the Bank ever provided the North Korean hackers or any of the conspirators with authority to access or remain on the Bank's networks.

366. These hacks interfered with the Bank's possessory interest in its networks and the information contained thereon.

367. Moreover, upon completing the hack by which the fraudulent payment orders were sent, the North Korean hackers destroyed and deleted numerous files across the network in an effort to cover their tracks, each an additional trespass upon and destruction of the Bank's property.

368. As noted above, civil conspiracy is a cognizable tort to the extent it alleges the existence of a conspiracy to connect the actions of the individual Defendants with an actionable, underlying tort, and establish that those actions were part of a common scheme.

369. Upon information and belief, the Defendants all entered into an agreement to participate in the scheme to break into the Bank's systems and launder funds obtained through illicit means from the United States and, therefore, Defendants are also liable for the civil conspiracy to commit the trespass against the Bank's property.

370. As a result, the Bank has suffered damages in the diminution of the value of its property and the costs necessary to repair the damaged property, plus other damages, including interest, attorneys' fees, and other damages, that may be proved at trial.

AS AND FOR A SEVENTH CAUSE OF ACTION

(Civil RICO Pursuant to 18 U.S.C. § 1962(c) Against All Defendants)

371. Plaintiff repeats and realleges the allegations contained in paragraphs 1 through 370 as if fully set forth below.

372. Plaintiffs and Defendants are all natural persons or legal entities, and as such are "persons" within the meaning of 18 U.S.C. § 1961(3).

373. The North Korean hackers, on the one hand, and the other Defendants, distinct groups of people, formed an enterprise within the meaning of 18 U.S.C. § 1961(4), with each Defendant being associated with the enterprise and forming an association in fact. The purpose of this enterprise was to steal the Bank's money and property from its bank account at the New York Fed located in New York City and to transport those stolen funds out of New York City and the United States, through the use of RCBC correspondent bank accounts in New York City, to the Philippines where the money was to be laundered through RCBC bank accounts and local casinos and questionable businesses. The Banking-Related Defendants provided the bridge between the Bank's account at the New York Fed in the United States and RCBC and casinos in the Philippines. The Casino-Related Defendants provided a route for the money to be further laundered and distributed to the thieves in and possibly outside of the Philippines. On information and belief, the enterprise and association in fact that made up the enterprise is made up of other individuals and entities, including the Doe Defendants, whose identities are not currently known.

374. Alternatively, the Banking-Related Defendants and the Casino-Related Defendants together constitute an enterprise within the meaning of 18 U.S.C. § 1961(4) with each Defendant

being associated with the enterprise and forming an association in fact. As stated above, at the time the lax anti-money laundering laws and exemption of casinos from those laws in the Philippines gave those defendants the ability to engage in their enterprise and, in this case, help steal and launder the Bank's funds. On information and belief, the enterprise and association in fact that made up the enterprise is made up of other individuals and entities, including the Doe Defendants, whose identities are not currently known.

375. Each of these enterprises engaged in, and their activities affected, domestic and international commerce, directed as they were to injuring the Bank in the United States by stealing its funds held at the New York Fed in New York City and then illegally transporting them outside the United States to the Philippines and potentially other international locations, and the laundering of those stolen funds first inside and then outside of the United States.

376. The enterprise also used four correspondent bank accounts at three intermediary banks located in the United States, three located in New York (and one in Philadelphia), to launder those funds through the Philippines. The enterprise did not merely utilize these banks to conceal or effectuate the theft, but also to steal the Bank's tangible property of $81,001,662.12 that was located in its specifically identifiable account at the New York Fed.

377. The pattern of racketeering consisted of and/or was further by, at least, the following predicate acts of the enterprise(s) in violation of law:

(a) 18 U.S.C. § 1029 relating to the use and trafficking with intent to defraud in one or more access devices and, in doing so, stealing the Bank's funds;

(b) 18 U.S.C. § 1343 relating to fraud by use of wire transmissions which caused the Bank's funds to be stolen out its bank account in New York;

(c) 18 U.S.C. § 1344 relating to bank fraud designed to steal the funds located in New York;

(d) 18 U.S.C. §§ 1956-1957 arising out of the laundering of the Bank's funds from its account at the New York Fed and to its ultimate recipients through the members of the enterprise(s);

(e) 18 U.S.C. §§ 2314-2315 relating to the transportation, receipt, and use of the stolen proceeds into foreign commerce and out of the United States by the members of the enterprise(s); and

(f) any state law predicate act such as theft, conversion, and robbery, which are the subject of the state law causes of action above.

378. More particularly, the enterprise violated 18 U.S.C. § 1029 — use and trafficking in access devices — by hacking into the Bank's systems and then using malicious software and falsified information, including access and log-in information, account numbers, SWIFT codes, electronic account information, and other means of obtaining unauthorized access to the Bank's SWIFT and other systems, which the enterprise used to send the fraudulent payment instructions, reach into the United States and a bank account therein, and steal, in a single day, $101 million ($20 million of which was returned) of the Bank's funds out of its New York Fed account.

379. Also, the enterprise violated 18 U.S.C. § 1343 — wire fraud — by utilizing the wire transfer network, and several American banks including the New York Fed from which the funds were stolen, inside the United States to effectuate the fraud. Indeed, the enterprise sent SWIFT instructions into the New York Fed, knowing and intending that the New York Fed would utilize the near instantaneous Fedwire system, maintained by the Federal Reserve, to transfer funds to three correspondent banks also in New York, which would in turn transfer those stolen funds from correspondent bank accounts held by RCBC, one of the members of the enterprise, at the American intermediary banks to the Fictitious Accounts in RCBC.

380. Also, the enterprise violated 18 U.S.C. § 1344 — bank fraud — by intentionally defrauding a financial institution — both the Bank and also the New York Fed from which the enterprise obtained the stolen proceeds — by sending the fraudulent payment instructions. As

noted above, the enterprise specifically directed the fraudulent payment instructions to the New York Fed, the leading bank of the American central bank, to steal the funds from the Bank out of the New York Fed and abusing the Fedwire system, along with the other intermediary banks, in furtherance of the theft. Indeed, eliminating any doubt as to the victims of this theft, in addition to the ultimate victim that was the Bank and its stolen funds, the hackers knowingly and intentionally listed the New York Fed and the three correspondent banks in New York in the fraudulent payment instructions.

381. The enterprise also violated 18 U.S.C. §§ 1956-1957 — money laundering and the use of laundered funds — as a core component of its scheme to steal the Bank's funds out of New York, transfer them through RCBC's correspondent accounts at the New York correspondent banks, then through SWIFT to RCBC, where the funds would be further laundered through numerous accounts, including the Fictitious Accounts and the Go-Centurytex Account, among others, and sent to the casinos where they would be further laundered and turned into clean, untraceable cash. This convoluted money laundering scheme was specifically designed to conceal and disguise the nature of the stolen funds, their location, source, ownership, and control, and did in fact do so, rendering significant portions of the stolen funds untraceable and which remain undiscovered to this date.

382. The enterprise also violated 18 U.S.C. §§ 2314-2315 — the transportation, receipt, and use of the stolen proceeds into foreign commerce and out of the United States —by spiriting the $101 million ($81 million upon return of one of the fraudulent payment instructions by the Sri Lankan bank) out of the United States, from the New York Fed, through Fedwire, to RCBC's possession in its correspondent accounts in the New York correspondent banks, then through SWIFT to the Fictitious Accounts at RCBC. From there, as set forth more fully above, the

Banking-Related Defendants engaged in a sophisticated web of transfers and foreign exchanges to transport and use the stolen proceeds, take their cut, and transfer them to the Casino-Related Defendants. Also as set more fully above, the Casino-Related Defendants utilized a similarly complex web of gamblers, casino junkets, specialized chips, and casino accounts to further transport, use, and launder the stolen proceeds, take their cut, and transfer the remaining funds to unknown recipients, the Doe Defendants.

383. Defendants' actions formed a related and continuous pattern of racketeering activity, which each of Defendants agreed to and did conduct. As shown above in Paragraphs 53-294, all of Defendants' actions were connected and had a singular unlawful purpose: to defraud, steal, and launder funds stolen from the Bank.

384. These actions occurred over a substantial period of time beginning with the North Korean hackers creation of the malware designed to gain access to the Bank's computer systems in 2014, the surveillance of the Bank's computer system over the course of 2015, the establishment of dollar accounts at RCBC specifically designed to receive and launder the funds stolen from the United States account of the Bank, and other potential victim banks, in July 2014, May 2015, December 2015, and February 2016, continuing with RCBC's actions laundering the funds through its correspondence accounts in the United States and within its own banking branches in the Philippines, culminating with the withdrawal of the funds to be moved to the casinos and to the wrongdoers.

385. The enterprise existed and operated before and after the theft of the funds from the Bank. According to the FBI and international experts, the same North Korean hackers tried similar heists from banks in Vietnam (TP Bank), the Philippines (not RCBC), Africa, Southeast Asia, Taiwan, India, Poland, Mexico, and South America (including Chile and Ecuador). NK Complaint

¶ 143, 189. Those illegal attacks were stymied (in part because of the lessons learned from the Bank's misfortune and losses), but demonstrate that the enterprises illegal activity extended beyond the attack on the bank to other potential victims for the common purpose of stealing funds from banking institutions well into 2018 if not the present. *Id.*; Lucinda Shen, *North Korea Has Been Linked to the SWIFT Bank Hacks*, Fortune, May 27, 2016, http://fortune.com/2016/05/27/north-korea-swift-hack/; *India bank hack similar to Bangladesh Bank heist*, Dhaka Tribune, Feb. 18, 2018.

386. Likewise, as Symantec, BAE Systems, FireEye, and other leading international cybersecurity experts have concluded, the North Korean hackers had been honing their craft leading up to the attacks on the banks. Jose Pagliery and Charles Riley, North Korea-linked 'Lazarus' hackers hit a fourth bank in Philippines, CNN, May 27, 2016, https://money.cnn.com/2016/05/26/technology/swift-bank-hack-philippines-lazarus/; Nicole Perltroth and Michael Corkery, *North Korea Linked to Digital Attacks on Global Banks*, N.Y. Times, May 26, 2016, https://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html?_r=0 (quoting experts at Symantec that "[w]e've never seen an attack where a nation-state has gone in and stolen money"); Dustin Volz & Jeremy Wagstaff, *Cyber firms say Bangladesh hackers have attacked other Asian banks*, Reuters, May 26, 2016, https://www.reuters.com/article/us-cyber-heist-swift-symantec/cyber-firms-say-bangladesh-hackers-have-attacked-other-asian-banks-idUSKCN0YH29J.

387. The "APT" designation given to the suspected group of North Korean hackers, also referred to as Lazarus Group or APT38, stands for "Advanced Persistent Threat," and such a designation "typically refers to attackers that wage long, sustained and stealthy attacks against preselected targets." Michael Schwartz, *North Korean Hackers Tied to $100 Million in SWIFT*

Fraud, BankInfo Security, Oct. 4, 2018, https://www.bankinfosecurity.com/north-korean-hackers-tied-to-100-million-in-swift-fraud-a-11579. This enterprise and the related pattern of racketeering was a grand, multi-year conspiracy to steal money and valuable information.

388. As noted above, including but not limited to Causes of Action One through Four, each person associated in fact with the enterprise had its role to play and profited from their participation in and association with the enterprise.

389. These Defendants have directly and indirectly conducted and participated in the conduct of the enterprise's affairs through the pattern of racketeering and activity described above, in violation of 18 U.S.C. § 1962(c).

390. As a direct and proximate result of the violations of 18 U.S.C. § 1962(c), Plaintiffs have been directly injured in their business and property at least in the full amount of the stolen funds as a direct result of the predicate acts intended to steal those funds, plus other damages, including interest, attorneys' fees, treble damages, and other damages, that may be proved at trial.

AS AND FOR AN EIGHTH CAUSE OF ACTION
(Unjust Enrichment Against All Defendants)

391. Plaintiff repeats and realleges the allegations contained in paragraphs 1 through 390 as if fully set forth below.

392. Regardless of their intent, many of the Defendants were also unjustly enriched from the scheme.

393. Each of the foregoing Defendants were enriched at the Bank's expense, which has not been able to recover the stolen funds and has expended significant resources in attempts to recover those funds.

394. Given the role of the Defendants in the conduct at issue in this case and as more fully described above, each Defendant's retention of the benefits of this massive fraud and theft

orchestrated against the Bank would be patently unjust, and equity and good conscience demands that each Defendant return any amount of gain obtained over the course of the scheme discussed herein to the Bank.

395. Unfortunately, because a significant portion of the funds stolen were secreted away, and these Defendants have been unwilling to assist the Bank or even disclose what each of their gains from the theft was, discovery is necessary to determine the full amount of unjustly retained funds by each Defendant.

396. Nonetheless, at the very least, Defendant RCBC made potentially hundreds of thousands or millions of dollars arising out of the numerous transfers within accounts held at RCBC, including foreign exchange fees on transfers with the RCBC Treasury, in an amount to be fully ascertained through discovery.

397. Similarly, Defendant Deguito personally withdrew and delivered cash payments in furtherance of the theft and money laundering scheme. Given that millions of dollars of cash were not used to purchase casino chips or laundered through the casinos, on information and belief, Defendant Deguito retained funds in an amount to be fully ascertained through discovery.

398. Defendants Philrem and the Bautistas also funneled funds through the various accounts at RCBC, including foreign exchange transfers, and were responsible for withdrawing and delivering cash payments in furtherance of the theft and money laundering scheme as well. According to Michael Bautista's own testimony, Philrem earned at least several hundred thousand dollars from its role in the fraud — and given the inconsistencies with his wife's, Salud Bautista's, testimony, on information and belief it is much more. Indeed, given that millions of dollars of cash were not used to purchase casino chips or laundered through the casinos, on information and

belief, Defendants Philrem and the Bautistas retained funds in an amount to be fully ascertained through discovery.

399. Defendants Centurytex and William So Go also opened and funneled funds through the various accounts at RCBC in furtherance of the theft and money laundering scheme as well. Given that millions of dollars of cash were not used to purchase casino chips or laundered through the casinos, on information and belief, Defendants Centurytex and William So Go retained funds in an amount to be fully ascertained through discovery.

400. Defendant Solaire Casino allowed highly suspicious amounts of cash to enter its casino, accepted on its premises by individuals with dubious claims and false identification, and then gamble away those funds while retaining for itself all of the profits from the gambling aspect of the money laundering operation. Solaire Casino has also seized approximately $2 million of funds from the gamblers that were laundering the funds that it has set aside in a frozen account and failed to pay over to the Bank. Between its profits on the gambling, which were, on information and belief, in the millions of dollars, and the $2 million of frozen funds, Solaire Casino is in possession of an amount of funds, in the millions of dollars, to be fully ascertained through discovery.

401. Defendants Eastern Hawaii Leisure and Kim Wong also allowed highly suspicious amounts of cash to enter the casino junkets they were running, despite that such funds were provided under highly suspicious circumstances by individuals unknown to them. Despite that they accepted approximately $21 million (and potentially as much as $35 million), Defendants Eastern Hawaii Leisure and Kim Wong have returned only $15 million even though it appears as though they did or should have stopped a much greater amount of those funds, calling into question where the remaining $6 million to $20 million or more is located. Moreover, Defendant Kim

Wong has indicated that he accepted at least some funds for the repayment of an antecedent debt, which is a benefit to Defendant Wong that should not be retained. Therefore, on information and belief, Defendants Eastern Hawaii Leisure and Kim Wong retained funds in an amount to be fully ascertained through discovery.

402. Defendants Ding Zhize, Weikang Xu, and Gao Shuhua each were involved in the delivery, acceptance, and gambling (laundering) of the funds withdrawn from the accounts at RCBC and placed in casino accounts and chips (or delivered as cash). Given that these individuals disappeared from the Philippines shortly after the casinos stopped their play (laundering) and that millions of dollars of cash were not used to purchase casino chips or laundered through the casinos, on information and belief, Defendants Ding Zhize, Weikang Xu, and Gao Shuhua retained funds in an amount to be fully ascertained through discovery.

403. Finally, John Does 1-25 constitute individuals and entities who may have been involved in the laundering of Plaintiff's funds, including but not limited to personnel of RCBC, the individuals responsible for opening the accounts at RCBC in the fictitious names of Cruz, Lagrosas, Vergara, and Vazquez, and any other individual or entity that was involved in the theft. Given that millions of dollars of cash remain missing, on information and belief, these John Doe Defendants retained funds in an amount to be fully ascertained through discovery.

AS AND FOR A NINTH CAUSE OF ACTION
(Money Had and Received Against All Defendants)

404. Plaintiff repeats and realleges the allegations contained in paragraphs 1 through 403 as if fully set forth below.

405. Regardless of their intent, many of the Defendants also received money rightly belonging to the Bank, and have benefited from the receipt of that money.

406. Given the role of the Defendants in the conduct at issue in this case and as more fully described above, each Defendant's retention of the benefits of this massive fraud and theft orchestrated against the Bank would defy principles of good conscience, and each Defendant should be required to return any money in its possession in connection with the theft of the Bank's funds.

407. Unfortunately, because a significant portion of the funds stolen were secreted away, and these Defendants have been unwilling to assist the Bank or even disclose what each of them currently hold, discovery is necessary to determine the full amount of unjustly retained funds by each Defendant.

408. Nonetheless, at the very least, Defendant RCBC retained potentially hundreds of thousands or millions of dollars arising out of the numerous transfers within accounts held at RCBC, including banking fees and foreign exchange fees on transfers with the RCBC Treasury, in an amount to be fully ascertained through discovery.

409. Similarly, Defendant Deguito personally withdrew and delivered cash payments in furtherance of the theft and money laundering scheme. Given that millions of dollars of cash were not used to purchase casino chips or laundered through the casinos, on information and belief, Defendant Deguito retained funds in an amount to be fully ascertained through discovery.

410. Defendants Philrem and the Bautistas also funneled funds through the various accounts at RCBC, including foreign exchange transfers, and were responsible for withdrawing and delivering cash payments in furtherance of the theft and money laundering scheme as well. Given that millions of dollars of cash were not used to purchase casino chips or laundered through the casinos, on information and belief, Defendants Philrem and the Bautistas retained funds in an amount to be fully ascertained through discovery.

411. Defendants Centurytex and William So Go also opened and funneled funds through the various accounts at RCBC in furtherance of the theft and money laundering scheme as well. Given that millions of dollars of cash were not used to purchase casino chips or laundered through the casinos, on information and belief, Defendants Centurytex and William So Go retained funds in an amount to be fully ascertained through discovery.

412. Defendant Solaire Casino allowed highly suspicious amounts of cash to enter its casino, accepted on its premises by individuals with dubious claims and false identification, and then gamble away those funds while retaining for itself all of the profits from the gambling aspect of the money laundering operation. Solaire Casino has also seized approximately $2 million of funds from the gamblers that were laundering the funds that it has set aside in a frozen account and failed to pay over to the Bank. These funds and any other funds in the possession of Solaire Casino, in amounts to be fully ascertained through discovery, should be returned to the Bank.

413. Defendants Eastern Hawaii Leisure and Kim Wong also allowed highly suspicious amounts of cash to enter the casino junkets they were running, despite that such funds were provided under highly suspicious circumstances by individuals unknown to them. Despite that they accepted approximately $21 million (and potentially as much as $35 million), Defendants Eastern Hawaii Leisure and Kim Wong have returned only $15 million even though it appears as though they did or should have stopped a much greater amount of those funds, calling into question where the remaining $6 million to $20 million or more is located. Therefore, on information and belief, Defendants Eastern Hawaii Leisure and Kim Wong retained funds in an amount to be fully ascertained through discovery.

414. Defendants Ding Zhize, Weikang Xu, and Gao Shuhua each were involved in the delivery, acceptance, and gambling (laundering) of the funds withdrawn from the accounts at

RCBC and placed in casino accounts and chips (or delivered as cash). Given that these individuals disappeared from the Philippines shortly after the casinos stopped their play (laundering) and that millions of dollars of cash were not used to purchase casino chips or laundered through the casinos, on information and belief, Defendants Ding Zhize, Weikang Xu, and Gao Shuhua retained funds in an amount to be fully ascertained through discovery.

415. Finally, John Does 1-25 constitute individuals and entities who may have been involved in the laundering of Plaintiff's funds, including but not limited to personnel of RCBC, the individuals responsible for opening the accounts at RCBC in the fictitious names of Cruz, Lagrosas, Vergara, and Vazquez, and any other individual or entity that was involved in the theft. Given that millions of dollars of cash remain missing, on information and belief, these John Doe Defendants retained funds in an amount to be fully ascertained through discovery.

WHEREFORE, Plaintiff seeks judgment as follows:

a) On Plaintiff's First Cause of Action, enter a judgment in favor of Plaintiff and against Defendants, jointly and severally, for all damages arising out of and as a result of Defendants' conversion, misappropriation, and theft of Plaintiff's property, in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, and other damages, to be determined at trial;

b) On Plaintiff's Second Cause of Action, enter a judgment in favor of Plaintiff and against Defendants, jointly and severally, for all damages arising out of and as a result of Defendants' aiding and abetting of conversion, misappropriation, and theft of Plaintiff's property, in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, and other damages, to be determined at trial;

c) On Plaintiff's Third Cause of Action, enter a judgment in favor of Plaintiff and against RCBC for all damages arising out of and as a result of the RCBC's commission of fraud, in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, and other damages, to be determined at trial;

d) On Plaintiff's Fourth Cause of Action, enter a judgment in favor of Plaintiff and against Defendants, jointly and severally, for all damages arising out of and as a result of Defendants' aiding and abetting fraud, in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, and other damages, to be determined at trial;

e) On Plaintiff's Fifth Cause of Action, enter a judgment in favor of Plaintiff and against Defendants, jointly and severally, for all damages arising out of and as a result of Defendants' conspiracy to convert, misappropriate, steal, or defraud Plaintiff, in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, and other damages, to be determined at trial;

f) On Plaintiff's Sixth Cause of Action, enter a judgment in favor of Plaintiff and against the Defendants, jointly and severally, for all damages arising out of and as a result of Defendants' participation in the conspiracy to trespass against Plaintiff's property and cause destruction and damage thereto, to convert, misappropriate, and steal Plaintiff's property, in the diminution of the value of its property and the costs necessary to repair the damaged property, plus other damages, including interest, attorneys' fees, and other damages, to be determined at trial;

g) On Plaintiff's Seventh Cause of Action, enter a judgment in favor of Plaintiff and against Defendants, jointly and severally, for all damages arising out of and as a result of Defendants' violation of 18 U.S.C. § 1962(c)

(Civil RICO), in the full amount of the stolen funds, plus other damages, including interest, attorneys' fees, treble damages, and other damages, to be determined at trial;

h) On Plaintiff's Eighth Cause of Action, enter a judgment in favor of Plaintiff and against each Defendants in the amounts each Defendant was unjustly enriched by his, hers, or its participation in the course of conduct resulting from the theft of Plaintiff's property, in amounts to be determined at trial;

i) On Plaintiff's Ninth Cause of Action, enter a judgment in favor of Plaintiff and against each Defendants in the amounts each Defendant had and received of Plaintiff's property, in amounts to be determined at trial; and

j) Award any other and further relief in favor of Plaintiff, including attorneys' fees and costs as available under applicable law, interest, and any such other and further relief as this Court deems just and proper.

Dated: New York, New York
January 31, 2019

Respectfully submitted,

COZEN O'CONNOR
Attorneys for Plaintiff

By: s/ John J. Sullivan__
John J. Sullivan, Esq.
Jesse Loffler, Esq.
Yehudah Gordon, Esq.
45 Broadway
New York, New York 10006
Tel: (212) 509-9400
Fax: (212) 509-9492
Email: jsullivan@cozen.com
Email: jloffler@cozen.com
Email: ygordon@cozen.com