FEDERAL DEPOSIT INSURANCE CORPORATION

WASHINGTON, D.C.

In the Matter of CBW Bank Weir, Kansas (Insured State Nonmember Bank) Respondent's NMLS UI# N/A	NOTICE OF ASSESSMENT OF CIVIL MONEY PENALTY, FINDINGS OF FACT AND CONCLUSIONS OF LAW, ORDER TO PAY, and PRAYER FOR RELIEF FDIC-22-0171k

The Federal Deposit Insurance Corporation (FDIC) has determined that CBW Bank, Weir, Kansas (Respondent or Bank), violated laws or regulations in conducting its affairs from on or about December 11, 2018, through on or about August 19, 2020 (Review Period). Specifically, Respondent failed to maintain an adequate Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) compliance program, which led to multiple incidents where Respondent repeatedly violated the Bank Secrecy Act (BSA), 31 U.S.C. § 5311 *et seq.*; 12 U.S.C. § 1829b; 12 U.S.C. §§ 1951–1960; 12 U.S.C. § 1818(s); and their implementing regulations, 31 C.F.R. Chapter X, 12 C.F.R. § 326.8 and 12 C.F.R. § 353. Further, Respondent's violations were part of a pattern of misconduct, and Respondent received financial gain or other benefit.

NOTICE OF ASSESSMENT OF CIVIL MONEY PENALTY

The FDIC issues this Notice of Assessment of Civil Money Penalty, Findings of Fact and Conclusions of Law, and Order to Pay (collectively, Notice of Assessment) under 12 U.S.C. § 1818(i)(2), and the FDIC Rules of Practice and Procedure, 12 C.F.R. Part 308, subparts A and

B. This proceeding assesses a $20,448,000 civil money penalty against Respondent under 12 U.S.C. § 1818(i)(2), unless Respondent formally objects by timely requesting a hearing under 12 U.S.C. § 1818(i)(2)(H).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

The FDIC makes the following allegations against Respondent:

I. Jurisdiction

1. Throughout the Review Period and continuing through the present day, Respondent was a corporation existing and doing business under the laws of the State of Kansas with its principal place of business in Weir, Kansas.

2. Throughout the Review Period and continuing through the present day, Respondent was an insured State nonmember bank, subject to 12 U.S.C. §§ 1811-1831aa, 12 C.F.R. Chapter III, and the laws of the State of Kansas.

3. Throughout the Review Period and continuing through the present day, Respondent is and was an "insured depository institution" as that term is defined in 12 U.S.C. § 1813(c)(2).

4. The FDIC is and was the "appropriate Federal banking agency" to maintain this enforcement action pursuant to 12 U.S.C. § 1813(q)(2).

5. The FDIC has jurisdiction over Respondent and the subject matter of this proceeding.

II. Respondent's AML/CFT Compliance Program Failed to Effectively Monitor and Manage Money Laundering/Terrorist Financing (ML/TF) Risk

6. During the Review Period, Respondent operated a multi-billion-dollar international money transfer business from its headquarters in Weir, Kansas, and an operations center located in Topeka, Kansas. Respondent provided banking to its mainly rural, retail customer base from the Weir location, but generated the bulk of its earnings from fee-based correspondent banking services for foreign financial institutions (FFIs).

7. During the Review Period, Respondent provided international banking services for more than 30 FFIs, at least six money services businesses (MSBs), and several other businesses providing financial services to individuals and entities in Central and South America, Europe, Africa, and the Middle East.

8. As part of these international banking services, Respondent performed U.S. dollar repatriation, cross-border remote deposit capture (RDC) for checks, correspondent banking for participants in the Sistema De Pagos Interbancarios en Dolares (SPID), and high-volume international electronic funds transfer via wires and Automated Clearing House (ACH).

9. During the Review Period, Respondent failed to create and maintain an AML/CFT compliance program commensurate with the elevated ML/TF risks of its business operations, as the FDIC documented in its 2019 BSA Examination, the resulting 2020 Consent Order, and subsequent examinations.

10. Specifically, Respondent failed to adequately provide for (1) a system of internal controls to assure compliance with the BSA, (2) independent testing of the AML/CFT

compliance program, (3) an adequately trained and empowered BSA officer to coordinate and monitor BSA compliance, and (4) BSA training for relevant personnel.

11. During the Review Period, Respondent also (1) failed to file hundreds of suspicious activity reports (SARs), (2) lacked an appropriate risk-based customer due diligence process, and (3) maintained an inadequate due diligence program for FFI correspondent accounts.

12. Due to the failures described above, Respondent earned millions in fee income that it otherwise would not have earned if it had maintained an adequate AML/CFT compliance program.

13. During the Review Period, Respondent did not expend the resources necessary to achieve a compliant AML/CFT compliance program, exaggerating increases in net income through reduced overhead.

14. The FDIC notified Respondent in a 2017 Report of Examination that Respondent's AML/CFT program had several deficiencies including in the areas of customer due diligence; BSA policies and procedures; BSA risk assessment; and independent testing.

15. As further detailed below and documented in the subsequent 2022 and 2023 Reports of Examination, Respondent has failed to correct many of the BSA issues described above.

III. Respondent Failed to Develop and Administer an Adequate AML/CFT Compliance Program in Violation of 12 C.F.R. § 326.8(b)(1)

16. Under 12 C.F.R. § 326.8(b)(1) all FDIC-supervised institutions must develop and provide for the continued administration of a written program reasonably designed to assure and monitor compliance with recordkeeping and reporting requirements set forth in 31 U.S.C.

Chapter 53, subchapter II, and the implementing regulations at 31 C.F.R. Chapter X (AML/CFT Compliance Program).

17. During the Review Period, Respondent failed to develop and provide for the administration of an adequate AML/CFT Compliance Program.

18. Under 12 C.F.R. § 326.8(c) FDIC-supervised institutions must (1) provide for a system of internal controls to assure ongoing compliance; (2) provide for independent testing for compliance; (3) designate one or more individuals responsible for coordinating and monitoring day-to-day compliance; and (4) provide training for appropriate personnel. Respondent's program met none of these requirements.

19. Since the Review Period, Respondent has continued to fail to develop and provide for the administration of an adequate AML/CFT Compliance Program.

A. Respondent's Internal Control System Was Weak and Ineffective

20. The BSA and its implementing regulations for FDIC-supervised institutions require banks such as Respondent to maintain an AML/CFT compliance program that includes "at a minimum" an internal control system "to assure ongoing compliance." 12 C.F.R. § 326.8(b).

21. Compliance programs should be "risk-based, including ensuring that more attention and resources" of a bank are "directed towards higher-risk customers and activities, consistent with" a particular bank's risk profile. 31 U.S.C. § 5318(h)(2)(B)(iv).

22. During the Review Period, Respondent's internal control system was not reasonably designed to assure and monitor BSA compliance, nor was it based on the risks presented by Respondent's customer base and services offered.

23. Since the Review Period and continuing through the present day, Respondent's internal control system is not reasonably designed to assure and monitor BSA compliance, nor is it based on the risks presented by Respondent's customer base and services offered, despite shifting to new business lines and developing a new customer base.

24. During the Review Period, Respondent's internal controls were deficient in its major business lines: U.S. dollar repatriation, international wire, and RDC.

25. Since the Review Period, the Respondent's internal controls remain deficient in relation to its new payment systems-based business lines.

26. During the Review Period, Respondent failed to perform adequate customer due diligence.

27. Since the Review Period, Respondent continues to fail to perform adequate customer due diligence.

U.S. Dollar Repatriation Services

28. Respondent provided U.S. dollar repatriation services during the Review Period, including millions of dollars in bulk cash shipments from Mexico for five Mexico-chartered banks and an MSB. Bulk cash shipments from Mexico are a major concern for U.S. law enforcement because they are often associated with money laundering in connection with drug trafficking activities.

29. Respondent completed more than $433 million in bulk currency shipments for Customer A, an FFI, during the Review Period.

30. During the Review Period, Respondent's internal control procedures for bulk cash consisted largely of an automated review utilizing an affiliate-developed AML/CFT monitoring

software named Context Engine, which was Respondent's primary AML/CFT tool to identify suspicious activity.

31. To commence use of the U.S. dollar repatriation service, institutional customers, including Customer A, would first send an initial cash sales report to Respondent prior to shipment. Respondent then used that customer-provided report to prepare Respondent's own version of the sales report, which consisted of manually reviewing the customer-provided report to ensure the data was in a format that could be uploaded to Context Engine. Respondent submitted its version of the report to Context Engine.

32. Respondent relied upon Context Engine to review this report for missing data, sales exceeding limits under applicable laws, duplicate transactions, transactions from the same or similar time and locations, customer identification documents, customers needing further identification, customer ages below 18 or above 90, and name matches from watch lists like the U.S. Office of Foreign Assets Controls (OFAC) Specially Designated Nationals and Blocked Persons list.

33. Despite Respondent's reliance on Context Engine, Respondent made a number of critical errors in using Context Engine that undermined the integrity of the review process. Respondent also failed to ensure it included necessary criteria in its manual and Context Engine-based reviews. For example, Respondent failed to include currency denominations in its manual bulk cash analysis. Also, Respondent's bulk cash shipment reports only compared expected amounts to actual amounts and did not contain any analysis of where the funds deposited were wired to or from, or the identity of wire counterparties to identify potentially suspicious patterns or activities.

34. As one example, Customer A's bulk cash business presented several red flags for ML/TF, but Context Engine did not flag the transactions. In 2018, Customer A wired over 70 percent of the bulk cash funds to accounts at a different FFI in Grand Cayman. In addition, Respondent's BSA Officer failed to independently review these transactions and was unaware they had occurred.

35. Prior to FDIC examiners questioning some of the transactions, Respondent never escalated a case for further investigation or filed a SAR on a bulk cash shipment.

International Wire Services

36. Respondent processed over $27 billion in wire transactions for FFIs in 2018 alone, and billions in other years as well. The Bank's total assets ranged from approximately $52 million to $120 million during the Review Period.

37. Many wires processed by Respondent through Context Engine were for FFIs in Mexico that participated in that country's SPID program, a U.S. dollar settlement program for Mexican banks run through Mexico's central bank. Respondent processed more than $13 billion in SPID transactions in 2018 and continued the activity throughout the duration of the Review Period. Respondent failed to monitor the settlement activity for ML/TF indicators and did not timely file any SARs on the SPID transactions.

38. During the Review Period, Respondent also provided correspondent wire services for FFIs located in or doing business in high-risk jurisdictions such as Lebanon, Brazil, and Cyprus.

39. In many instances, Context Engine failed to detect suspicious transactions, and, in some instances, when Context Engine did detect suspicious activity, Respondent failed to act.

40. After collecting information on a transaction, Context Engine generated a score for each transaction. If the score was 75 or above, Context Engine was intended to flag the transaction for review by an analyst. Respondent maintained no rationale or support for Context Engine's rules and their assigned risk weights; no identification or support for model changes, like removing or adding rules; and no explanation to address Context Engine's text search function and how it scored matches.

41. At the automated review level, Context Engine failed to detect many suspicious wire transactions. As an example, Context Engine failed to flag repeated cross-border transactions below the preset $10,001 threshold that Respondent had determined was the proper level for suspicious activity detection. Context Engine scenarios also ran only against individual transactions and did not screen for recurring patterns or aggregation.

42. Context Engine did not contain a ruleset to identify potential concentration accounts, accounts which combine multiple individual customer transactions into a single account for transaction purposes; this lack of a ruleset potentially disguised the identity of the ultimate originator or the purpose of an individual transaction.

43. At the human review level, Respondent tasked only four analysts to review thousands of daily wires that Context Engine flagged. Respondent repeatedly failed to detect or report suspicious activity in wires flagged for manual review.

44. Respondent also failed to consider how institutional wire customers utilized concentration accounts to initiate transfers between low and high-risk jurisdictions.

45. For example, Customer B, an FFI, was based in the United Kingdom, which Respondent graded as a low-risk jurisdiction. However, Respondent failed to recognize that

Customer B was using concentration accounts to originate wires for its customers with direct ties to high-risk jurisdictions and did not appropriately monitor that activity.

46. Customer B used account numbers for five originators and one beneficiary to process more than 5,000 wire transactions for hundreds of different entities totaling $400 million over an eight-month period.

47. Customer B used concentration accounts to transmit those wires on behalf of international money transmitters and foreign exchange companies to countries in South America.

48. Due to Respondent's failure to appropriately flag concentration accounts, Respondent failed to monitor these wire transactions. Customer B's wire transactions also included suspicious activity indicators such as multiple transfers to the same entities on the same days and the use of nested accounts. Respondent failed to file SARs on these transactions.

49. Since the Review Period, despite being advised of Context Engines's failures to accurately identify suspicious transactions, Respondent continues to rely upon Context Engine.

RDC Services

50. Respondent processed approximately $461 million in RDC transactions in 2018 with additional transactions continuing through the Review Period. In the first quarter of 2019, Respondent processed more than 39,000 checks totaling over $134 million for a mix of institutional clients including FFIs and MSBs.

51. During the Review Period, Respondent relied on a hybrid of manual processes and Context Engine to screen RDC transactions for potential ML/TF risk.

52. Respondent's institutional RDC customers—mainly FFIs and MSBs—submitted check images from individuals and businesses to Respondent for processing. Despite originating almost exclusively from non-U.S. locations, all checks were drawn on U.S.-based institutions.

53. In the manual review process, operational employees reviewed submissions for errors, missing information, or items Respondent did not accept. Employees also reviewed the data for items that could require prior approval, such as checks over $10,000. This review inappropriately focused on operational issues rather than ML/TF red flags.

54. Respondent also employed a specialized Context Engine program called "Check Machine" to review customer-provided sales reports on at least a monthly basis to monitor for ML/TF indicators. A Respondent employee then used that information to prepare a second report the BSA officer reviewed.

55. Context Engine's "Check Machine" program, which was entirely retrospective, only analyzed transactions by institution within a given month, and the program did not account for either individual customers using multiple institutions or individual customers using multiple services from the same institution.

56. During the Review Period, Respondent failed to identify red flags in multiple RDC transactions. These red flags included multiple even-dollar checks to the same payee, large checks posted to the same account multiple times a day, and multiple checks from the same maker under reporting thresholds, with many of the transactions occurring on consecutive days or the same day.

57. During the Review Period, Respondent also failed to effectively monitor the business purpose provided by the customer, and Respondent processed checks where the size, volume, and transaction details were inconsistent with the business purpose information provided

by the customer. In some instances, Respondent's analysts flagged transactions for review, but Respondent nonetheless failed to appropriately file SARs.

Customer Due Diligence

58. During the Review Period, Respondent failed to establish and maintain an effective customer due diligence program. For example, the BSA Officer's ongoing due diligence for Respondent's bulk cash business consisted only of comparing actual to expected cash deposits, without conducting a denomination analysis or monitoring customer activity on outgoing wires, causing Respondent to miss data that indicated ML/TF risk.

59. During the Review Period, Respondent also failed to perform any meaningful analysis of data collected from current and prospective FFI and MSB customers. While Respondent collected information like beneficial ownership declarations, articles of incorporation, service contracts, audits, and financial reports, Respondent performed limited independent due diligence on customers.

60. Since the Review Period, Respondent continued the practice of limited independent due diligence on new customers and expanded business lines at least through 2022.

B. Respondent Failed to Perform Sufficient Independent Testing

61. During the Review Period, Respondent employed external auditors in its attempt to meet the requirement for independent BSA compliance testing. However, the testing was too limited and lacked sufficient detail in connection with the testing methods and data for the tests to provide a meaningful evaluation of Respondent's AML/CFT compliance program.

62. For example, the auditor's 2019 independent testing scope of work stated it covered higher-risk business lines, including correspondent banking for FFIs, U.S. dollar repatriation, international wires, and MSB services.

63. However, the auditor's independent testing scope of work severely lacked depth and breadth of review. The auditor only sampled 10 wires for review despite Respondent processing in excess of 60,000 wires in 2018. Further, the auditor did not test any RDC transactions. The auditor also limited its suspicious activity review to ten cases where Respondent filed a SAR and three where Respondent decided not to file after review. In addition, the auditor only assessed transactions that Respondent itself elevated for a SAR filing review.

64. Since the Review Period, Respondent's independent testing deficiencies have continued.

C. Respondent's BSA Officer Was Ineffective and Was Not Provided Sufficient Support and Resources

65. Banks must designate "an individual or individuals responsible for coordinating and monitoring day-to-day [BSA] compliance." 31 C.F.R. § 1020.210(a)(2)(iii). A bank can fulfill this requirement if its board appoints a BSA Officer who can demonstrate their competence through their knowledge of the BSA and its related regulations, their implementation of the bank's AML/CFT compliance program, and their understanding of the ML/TF risk profile associated with the bank's activities.

66. The bank's board must also give the BSA officer the tools to administer the AML/CFT compliance program based on the bank's ML/TF risk profile, including appropriate authority, independence, and access to resources.

67. During the Review Period, Respondent had two different BSA Officers. BSA Officer A served from August 2018 until February 2020, and BSA Officer B served from February 2020 until June 2023.

68. During the Review Period, Respondent's BSA Officers lacked the experience necessary to manage the risks inherent in Respondent's business lines and customer base. In addition, Respondent did not grant its BSA Officers the authority, independence, and access to resources required by a BSA program commensurate with the ML/TF risks present in the Bank's business model and customer base.

69. Respondent's BSA Officer A had no prior banking or BSA officer experience.

70. Due to inadequate training and experience, Respondent's BSA Officer A was unfamiliar with basic concepts such as concentration account risks and failed to monitor customer accounts for suspicious activity in wires. Respondent's BSA Officer A also failed to recognize key indicators of ML/TF, including high-velocity transactions, potential structuring, and large transaction volumes with multiple counterparties in high-risk geographic jurisdictions.

71. Respondent's BSA Officer A admitted to the FDIC he was not qualified for the role when hired, and he relied on Respondent's Vice-President of Correspondent Banking, who was responsible for managing customer relationships, to understand Respondent's business lines.

72. In addition, Respondent's BSA Officers A and B lacked the authority, independence, and resources to adequately manage Respondent's AML/CFT compliance program. BSA Officer A told the FDIC that he was as concerned with losing a customer as he was with identifying and reporting suspicious activity.

73. Respondent also established personnel reporting lines that presented additional authority and independence weaknesses. During the Review Period, key AML/CFT monitoring

staff located in the continental U.S. reported to Respondent's cashier, rather than directly to the BSA Officer. Respondent also had AML/CFT monitoring staff in India and Puerto Rico, who reported to an individual titled Head of Offshore Operations.

74. Respondent's BSA Officer A admitted to the FDIC that he did not have unilateral authority to file a SAR. Rather, Respondent maintained a committee that reviewed and discussed whether to file SARs on flagged transactions. The committee's composition included the BSA Officer, the VP/Cashier, the VP of Correspondent Banking, and the President of the Bank. The committee did not include any outside board members. BSA Officer A told the FDIC while he should have retained the ultimate authority to file SARs, the committee made SAR filing decisions collectively, and the committee members would often rely on the Bank's VP of Correspondent Banking's explanations for why a transaction did not require a SAR.

75. During the Review Period, Respondent failed to provide its BSA Officers with the resources required to carry out their job duties. The BSA Officers relied heavily on Context Engine, which used Bank-developed scenarios to flag thousands of transactions. Despite the volume of flagged transactions, most scenarios did not directly relate to ML/TF risks.

76. Because Context Engine did not specifically identify ML/TF risks in its scenarios, individual analysts had to manually review the transactions to identify suspicious activity. Those analysts who were tasked with reviewing the flagged transactions lacked experience or expertise in identifying ML/TF risks.

77. Despite these weaknesses, Respondent continued to conduct millions of dollars in transactions each month during the Review Period for customers in multiple foreign countries. Respondent also continued to grow its high-risk customer base by seeking new international customers.

78. Since BSA Officer B's departure, Respondent has employed two additional BSA Officers. BSA Officer C served from June 2023 until November 2023, and BSA Officer D has served from January 2024 forward.

79. Respondent's BSA Officer issues have continued through the tenures of BSA Officers C and D. Neither was provided the authority, independence, or resources to improve Respondent's AML/CFT compliance program.

80. Respondent's current BSA Officer, BSA Officer D, lacks the experience and independence required to coordinate and monitor Respondent's BSA compliance in the current business lines and customer base.

D. Respondent's BSA Training Was Inadequate

81. During the Review Period, Respondent's BSA training had significant gaps given Respondent's high-risk, high-volume, international money transfer business. While records reflect that Respondent's staff received periodic training on AML/CFT compliance, that training lacked instruction on the advanced topics necessary given the risk level and volume of Respondent's activities.

82. Since the Review Period, training problems continued into at least 2022, as Respondent's BSA training program was neither sufficiently complex nor adequately tailored to the Respondent's activities or its risk profile.

IV. Respondent Failed to File Hundreds of SARs in Violation of 12 C.F.R. § 353.3

83. Respondent failed to file SARs during the Review Period on many occasions where Respondent "suspected" or "had reason to suspect" the transactions conducted or attempted by, at, or through the Bank (1) "involved funds derived from illegal activities" or were

"intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation"; (2) "were designed to evade any requirements of this chapter or of any other regulations promulgated under the Bank Secrecy Act"; or (3) had "no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage," and Respondent knew of "no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction." 12 C.F.R. § 353.3(a); 31 C.F.R. § 1020.320 (a)(2).

84. The President of the Bank told FDIC examiners that Respondent needed to keep its customers' interests in mind when considering whether to file SARs.

85. During the Review Period, Respondent failed to file SARs within the maximum 60 calendar days after initial detection as required by 12 C.F.R. § 353.3(b).

86. After the Review Period and through at least 2023, Respondent still failed to file required SARs on transactions which occurred during the Review Period that were conducted or attempted by, at or through the Bank.

V. Respondent's Customer Due Diligence Program Was Inadequate in Violation of 31 C.F.R. § 1020.210(b)(5)

87. While Respondent collected information from and on its customers during the Review Period, the information Respondent gathered was superficial and insufficient to understand "the nature and purpose of customer relationships for the purpose of developing a customer risk profile" and conduct "ongoing monitoring to identify and report suspicious

transactions and, on a risk basis, to maintain and update customer information." 31 C.F.R. § 1020.210(b)(5).

88. Examples of customer due diligence failures during the Review Period relate to Customer C and Customer D, both MSBs. Both customers frequently wired large round dollar amounts for individual customers. Respondent's due diligence did not include any analysis of the nature and purpose of the individual transactions. In the first quarter of 2019, Respondent processed more than 44,000 remittances in excess of $22 million for Customers C and D. The volumes did not align with the customers' expected activity levels.

89. Further, Respondent failed to identify signs of possible ML/TF risk in transactions for MSB Customer C, including dozens of even-dollar RDC transactions totaling approximately $135,000 and 18 cash remittances of approximately $1.4 million, all labeled "Regular Deposits"; and almost three dozen even-dollar outgoing international wires totaling more than $2 million, with several on the same day or consecutive days.

90. Respondent failed to identify similar indicators of suspicious activity for Customer D during the Review Period. For example, in June 2019, transaction records showed more than 100 deposits exceeding $8 million and 20 outgoing international wires of almost the same amount.

91. Respondent did not maintain, and could not produce upon request, documentation to support Customer C's or Customer D's activity levels. Any documentation Respondent maintained was superficial and lacked meaningful activity analysis.

92. During the Review Period, Respondent's customer due diligence program lacked meaningful review processes for FFIs. For example, Customer E utilized the Respondent's international wire services to transmit hundreds of millions of dollars. Respondent's initial

customer due diligence on Customer E, an FFI, acknowledged in 2016 that the former chairman of Customer E "allegedly had connections to Hezbollah," but went on to state that the individual no longer had "any role in the management or ownership of" Customer E. A 2019 report summarizing ongoing customer due diligence on Customer E prepared by Respondent failed to identify that OFAC added Customer E's former chairman to OFAC's Specially Designated Global Terrorist list in 2015, and that the former chairman transferred his ownership interests to one of his children. Under such a transfer, the former chairman was still an "owner" of Customer E.

93. Respondent also failed to identify negative news related to Customer E. The 2019 report failed to identify a news story on a lawsuit against Customer E over alleged ties to Hezbollah, instead stating, "[t]here were no material negative news stories about Customer E in the past twelve months."

94. Respondent's failure to maintain an adequate customer due diligence program during the Review Period constituted a violation of 31 C.F.R. § 1020.210(b)(5). Following the Review Period, this failure continued into at least 2022 as Respondent entered new business lines and acquired new customers.

VI. Respondent's Due Diligence Program for FFI Correspondent Accounts Was Inadequate in Violation of 31 C.F.R. § 1020.620

95. Respondent's due diligence program for FFI banking relationships failed to detect and report suspected ML/TF activity during the Review Period.

96. Respondent is required to have appropriate, specific, risk-based procedures reasonably designed to detect and report potential suspicious activity through any correspondent

account Respondent "established, maintained, administered, or managed" in the U.S. for an FFI. 31 C.F.R. § 1020.620 (cross-referenced to § 1010.620).

97. During the Review Period, Respondent's primary FFI wire transaction due diligence tool was a periodically signed statement from the FFIs about expected account activity. Respondent's procedures failed to recognize suspicious activity in many instances. Respondent violated 31 C.F.R. § 1020.620 by failing to conduct adequate due diligence on FFIs that received correspondent banking services.

VII. Conclusions of Law

98. Based on the misconduct described above, Respondent violated laws and regulations under 12 U.S.C. § 1818(i)(2).

99. Based on the misconduct described above, Respondent recklessly engaged in unsafe or unsound practices in connection with the Bank under 12 U.S.C. § 1818(i)(2).

100. Respondent's violations and practices were part of a pattern of misconduct under 12 U.S.C. § 1818(i)(2).

101. Respondent's violations and practices resulted in Respondent's financial gain or other benefit under 12 U.S.C. § 1818(i)(2).

ORDER TO PAY

Based on the above Findings of Fact and Conclusions of Law, the FDIC determined that Respondent's violations merit a civil money penalty. Taking into account the appropriateness of the penalty with respect to the following mitigating factors under 12 U.S.C. § 1818(i)(2)(G): size of Respondent's financial resources and good faith, the gravity of the violation(s), the history of previous violations, and such other matters as justice may require, it is:

ORDERED that, by reason of Respondent's violations listed above, a $20,448,000 penalty is assessed against CBW Bank, Weir, Kansas, under 12 U.S.C. § 1818(i)(2).

FURTHER ORDERED that the Order to Pay is stayed until 20 days after the date of service of this Notice of Assessment to allow Respondent time to object to the Order to Pay.

If Respondent wants to object to the Order to Pay, Respondent must formally request a hearing in writing within 20 calendar days after service of this Notice of Assessment, as explained at 12 U.S.C. § 1818(i)(2)(H). Respondent may object to the Order to Pay by requesting a hearing in a formal answer, as specified in 12 C.F.R. § 308.19. **If Respondent fails to request a hearing to object to the Order to Pay within 20 calendar days from the date of service of this Notice of Assessment, the penalty assessed against Respondent will be final and unappealable under 12 U.S.C. § 1818(i)(E)(ii) and 12 C.F.R. § 308.19(c)(2) and must be paid within 60 calendar days after the date of service of this Notice of Assessment.**

If Respondent timely requests a hearing, the hearing will be held before an Administrative Law Judge (ALJ) assigned by Office of Financial Institution Adjudication (OFIA) under 5 U.S.C. § 3105. The hearing on the Order to Pay will begin on a date set by the ALJ in Kansas City, Kansas, or in another location set by the ALJ. The hearing will be public and conducted in accordance with 12 U.S.C. §§ 1811-1831aa, the Administrative Procedure Act, 5 U.S.C. §§ 551-559, and 12 C.F.R. Part 308, subparts A and B.

An original and one copy of all papers filed in this proceeding must be served upon OFIA, 3501 N. Fairfax Drive, Suite VS-D8116, Arlington, Virgina 22226-3500, in the manner specified at 12 C.F.R. § 308.10. Copies of all papers filed in this proceeding must be served upon the following: FDIC Administrative Officer, 550 17th Street, N.W., Washington, D.C. 20429;

Seth P. Rosebrock, Assistant General Counsel, Frank Salomone, Senior Counsel, and Sam Ozeck, Supervisory Counsel, Enforcement Section, Legal Division, FDIC, 550 17th Street, N.W., Washington, D.C. 20429; Sonya Allen, Regional Counsel and J. Spencer Culp, Senior Regional Attorney, FDIC, 1100 Walnut Street, Ste. 2100, Kansas City, Missouri 64106. Respondent is encouraged to file any subsequent documents electronically with OFIA at ofia@fdic.gov.

PRAYER FOR RELIEF

The FDIC prays that an Order to Pay in the amount of $20,448,000 and assessed under 12 U.S.C. § 1818(i)(2), be issued against Respondent.

Issued under delegated authority.

DOREEN EBERLEY Digitally signed by DOREEN EBERLEY Date: 2024.11.18 13:43:25 -05'00'

Doreen R. Eberley
Director
Division of Risk Management Supervision