EXHIBIT 49

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

BLUE FLAME MEDICAL LLC *Plaintiff*, v. CHAIN BRIDGE BANK, N.A., JOHN J. BROUGH, and DAVID M. EVINGER, *Defendants.*	)	Civil Action No. 1:20-cv-00658
CHAIN BRIDGE BANK, N.A. *Third-Party Plaintiff*, v. JPMORGAN CHASE BANK, N.A. *Third-Party Defendant*.	)	

REBUTTAL EXPERT REPORT OF SEAN O'MALLEY
ON BEHALF OF PLAINTIFF BLUE FLAME MEDICAL LLC

MARCH 12, 2021

TABLE OF CONTENTS

I. Scope of Assignment

I have been asked by Schulte Roth & Zabel LLP ("Counsel") on behalf of its client, Blue Flame Medical LLC ("Blue Flame Medical"), to respond to the opinions set forth in the Expert Report of Charles H. Grice, dated February 12, 2021 (the "Grice Report").[1] I reserve the right to supplement my opinions should I become aware of additional facts or information, if Mr. Grice clarifies or changes his opinions, or if I am asked to perform additional analyses.

II. Qualifications

As with my initial expert report in this matter, dated February 12, 2021 ("Initial Report"), the issues on which I have been asked to provide opinions concern topics that I have regularly encountered over my career in working for and advising multinational banking institutions. I have worked in the banking and financial services industry for over 30 years, specializing in Anti-Money Laundering ("AML"), operational risk management and compliance. I have had extensive involvement in the development and enhancement of anti-money laundering programs at two different global banks, Citigroup Inc. and State Street Bank. In that capacity, I have led teams dealing with risk analytics, model risk management, risk assessment, data governance and data acquisition. I have been responsible for Comprehensive Capital Analysis Review ("CCAR") / Dodd-Frank Act Stress Tests ("DFAST") capital models. In AML I have developed enterprise-wide risk methodologies for country risk (globally), product risk and customer risk for global banks.

[1] Mr. Grice issued two identically titled reports dated February 12, 2021; one is 59 pages in length and the other is 11 pages. The "Grice Report" referenced herein is the 59-page report issued by Mr. Grice.

I am a Managing Director at Integrated Risk, LLC, an enterprise risk management consultancy with a focus on Anti-Money Laundering and Compliance, where I am currently engaged in a consulting role to a foreign bank organization as the head of their financial investigation unit, and have also worked on engagements to optimize transaction monitoring scenarios for Citigroup. Prior to founding Integrated Risk, LLC in 2019, I served as the Global Head of Anti-Money Laundering Risk Management at State Street Bank from June 2015 through May 2019, where I was responsible for its anti-money laundering customer risk rating methodology, enterprise-wide anti-money laundering risk assessments, and enterprise-wide sanctions risk assessments. I also served as a member of its financial intelligence unit oversight committee. Prior to that, I served as the U.S. Head of Operational Risk Modeling & Analytics at Santander Bank, N.A. from March 2014 through June 2015, with responsibility for the CCAR/DFAST analysis and loss estimates for operational risk. From September 2010 through March 2014, I was the Director of Compliance Analytics at Citigroup, and was responsible for developing its first globally-consistent anti-money laundering customer risk rating methodology and enterprise-wide anti-money laundering risk assessments, as well as serving as its global data governance officer for Compliance. I joined Citigroup from Morgan Stanley, where I served as an Executive Director of Operational Risk from November 2009 through September 2010. I worked at RVI Group where I was responsible for rating agency capital modeling and managing the credit default swap portfolio. At Financial Security Assurance, I was responsible for rating agency capital modeling, derivatives valuation and counterparty exposure reporting. I worked at Deloitte & Touche in the Capital Markets consulting team and managed the Security Markets Pricing Service for the Americas. I began my post-MBA career in the financial industry at Ford Motor Credit Company LLC, where I served as the Balance Sheet Manager in its Corporate Treasury Department from June 1996 to July 1997. Prior to earning my MBA, I worked at Federated Investors, Business & Estate Advisors, American Express Financial Services and Teacher's Federal Credit Union.

I have provided expert consulting and analysis in matters related to the banking and financial services industry. Specifically, I served as an expert witness in the municipal bond defeasance (also known as "yield burning") litigation for the law firm representing Merrill Lynch.

I earned a Master of Business Administration degree with concentrations in Finance, International Business and Strategy from the Tepper School of Business at Carnegie Mellon University (where I also served as President of the Finance Club) and a Bachelor of Sciences in Economics from the University of Minnesota. I hold the Certified Anti-Money Laundering Specialist ("CAMS") designation from the Association of Certified Anti-Money Laundering Specialists ("ACAMS"), the largest international anti-money laundering and financial crime prevention community worldwide.

III. Compensation

I have been retained by Counsel through an expert search firm, which is compensated for my time spent in this matter at a rate of $700 per hour. The fees paid are not contingent on the outcome of this matter. All opinions set forth in this report are my own.

IV. Facts and Data Considered

In connection with the preparation of this rebuttal report, I considered documents and information produced in this litigation, information obtained from my research, and my own knowledge and experience. Appendix A contains a listing of the documents and other information I have considered in forming the opinions set forth in this report, as well as the documents and other information I previously reviewed in connection with my Initial Report. Should additional information become available between now and trial, I will consider that information and update my opinions as necessary.

V. Summary of Opinions

In my opinion, the following enumerated "opinions" contained in the Grice Report are flawed, misleading, irrelevant, and/or simply wrong:

- Opinion No. 1: The wire transfer from the State of California to Chain Bridge Bank for the benefit of Blue Flame Medical exhibited characteristics of potentially suspicious activity.[2]
- Opinion No. 2: Actions taken by Chain Bridge Bank after opening Blue Flame Medical's account and receiving the wire transfer from the State of California were reasonable and consistent with industry standards.[3]

My difference in opinions from Mr. Grice, particularly concerning actions that he describes as "reasonable and consistent with industry standards and practices," may be attributable in part to our differing backgrounds. While Mr. Grice professes to be an expert in the area of Bank Secrecy Act ("BSA") and Anti-Money Laundering regulations and other banking regulations, and claims to have consulted and advised banks on those issues,[4] he evidently has

[2] Grice Report ¶ 16.
[3] Grice Report ¶ 16.
[4] Grice Report ¶ 3-4.

no first-hand experience working in Anti-Money Laundering compliance for commercial accounts as a member of any financial institution.

The experience Mr. Grice professes to have in the financial services industry also appears to be somewhat dated. Since his time at Kroll in risk consulting concluded in 2006, prior to the Financial Crisis, there have been significant changes in regulatory regimes and vigilance attributable to BSA and Anti-Money Laundering regulation and enforcement in the United States. Finally, he does not appear to possess a Certified Anti-Money Laundering Specialist (CAMS) certification, which is required of many Anti-Money Laundering professionals in banking today. Unlike Mr. Grice, I have worked continuously at major financial institutions for the majority of my professional career, including in an in-house capacity as recently as 2019 prior to my moving into my current consulting role, and have spent years devoted to Anti-Money Laundering monitoring, compliance, and risk analysis concerning large financial transactions for commercial accounts.

VI. Specific Responses to Mr. Grice's Opinions

A. Response to Grice Opinion No. 1

Mr. Grice's opinion that the wire transfer from the State of California to Chain Bridge Bank exhibited characteristics of potentially suspicious activity is flawed and misleading. His opinion ignores the record in this case concerning Chain Bridge Bank's awareness of key facts in connection with Blue Flame Medical's business and the Wire Transfer,[5] and exaggerates certain facts in an effort to help justify Chain Bridge Bank's actions. His opinion also relies on

[5] Terms defined in my Initial Report have the same meaning in this report.

conclusions that are flatly wrong and which I do not believe are consistent with standard banking industry and Anti-Money Laundering practice.

Mr. Grice bases his opinion on his findings regarding the following issues:

a) Blue Flame Medical was a newly formed entity and the principals were "unable to furnish requested documentation" to Chain Bridge Bank;

b) The wire transfer from the State of California to Blue Flame Medical was outside of expected activity for Blue Flame Medical's account;

c) Blue Flame Medical's principals and employees exhibited "unusual and suspicious behavior";

d) Blue Flame Medical's transaction with the State of California was a "high velocity transaction";

e) Blue Flame Medical's transaction with the State of California involved "high risk jurisdictions"; and

f) JPMorgan Chase had communicated "concerns of fraud" regarding the Wire Transfer to Chain Bridge Bank.[6]

Based on my experience as an Anti-Money Laundering professional, I do not believe these factors—when viewed in their totality and in context with other key information known to Defendants on March 26, 2020—support Chain Bridge Bank's claim that its reversal of the Wire Transfer was motivated by concerns regarding suspicious activity or Anti-Money Laundering issues. Rather, as stated in my Initial Report, I believe that Chain Bridge Bank's decision to cause the return of the funds to JPMorgan Chase on March 26 was motivated by its concerns about the effect of a $456 million deposit on the bank's business, including its debt-to-equity ratio, rather than actual suspicious activity or Anti-Money Laundering concerns. Moreover, concerns regarding suspicious activity or Anti-Money Laundering issues—even if held in good

[6] *See* Grice Report ¶ 75.

faith—would not justify Chain Bridge Bank's request to JPMorgan Chase to recall the funds it had accepted and credited to Blue Flame Medical's account and agreement to the recall request by JPMorgan Chase that Chain Bridge Bank triggered.

i. Chain Bridge Bank was aware of Blue Flame's status as a newly formed entity when opening Blue Flame's account and the bank's stated desire to obtain documentation regarding Blue Flame Medical's contracts does not appear to have motivated its actions.

Mr. Grice's opinion relies heavily on his assessment that Blue Flame Medical was a newly formed entity with a new account and his belief that its principals were "unable to furnish requested documentation."[7] However, based on my experience and review of the record, I do not believe that those factors justified Chain Bridge Bank's apparent conclusion that the Wire Transfer or Blue Flame Medical were suspicious from a BSA or Anti-Money Laundering perspective. In any event, it does not appear that a lack of "documentation" concerning Blue Flame Medical's contract with the State of California factored into Chain Bridge Bank's decision to return the funds it accepted on Blue Flame Medical's behalf in connection with the Wire Transfer, as Chain Bridge Bank had received confirmation from California that such a contract existed before it decided to return the funds.

While it is true that Blue Flame Medical was a newly formed entity in late March of 2020, that fact was known to Chain Bridge Bank when it agreed to open Blue Flame Medical's account.[8] Based on my experience, any concerns about Blue Flame Medical's identity or legitimacy should and would have been investigated by Chain Bridge Bank as part of the account opening process, which at all banks includes customer due diligence. One of the

[7] *See* Grice Report ¶¶ 76-83.
[8] *See* Grice Report ¶ 27, n.34.

central elements of customer due diligence is a bank's Customer Identification Program ("CIP"), through which a bank seeks to confirm the identity of the customer. As part of a CIP, the customer's identity/name would be run through a series of searches to determine if there are any applicable sanctions concerns, negative news, or exposure to a politically exposed person ("PEP") or PEP-controlled entity. Additional information about the customer would be collected and used to determine both the customer's risk rating and an appropriate frequency for periodic review of the customer's risk profile—which is typically done no more frequently than semi-annually, even for newly established customers that are considered "high risk." The factors bearing on a customer's risk rating include jurisdictional/geographic risk of the customer, the customer's source of funds, nature of the customer's business, ownership structure (if the customer is a business organization) and expected activity. It is typical for a bank to conduct enhanced due diligence on a customer considered high risk due to some combination of customer risk rating factors.

Thus, Chain Bridge Bank would have considered Blue Flame Medical's status as a newly formed entity during the account opening process in order to determine the company's Anti-Money Laundering risk rating, periodic review frequency, and any additional due diligence requirements. In addition, the principals of Blue Flame Medical had opened new accounts with Chain Bridge Bank for other business organizations earlier in March 2020, for which Chain Bridge Bank would have performed a similar, and perhaps identical, customer due diligence process. Critically, if Chain Bridge Bank's customer due diligence process had raised concerns about Blue Flame Medical, its principals, or the other accounts its principals had opened at Chain Bridge Bank, the bank was free to refuse to open an account for Blue Flame Medical.

Because Chain Bridge Bank instead opened the account, it accepted Blue Flame Medical as a customer, along with any risk associated with its recent formation.

Similarly, Mr. Grice observes that under the Federal Financial Institution Examination Council ("FFIEC") BSA/AML Manual, one basis for finding a transaction potentially suspicious is when "[a] business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location."[9] Based on my review of relevant documents, I am not aware of any intentional omission by Blue Flame Medical of information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information regarding its business location. Moreover, based on my experience as an Anti-Money Laundering professional who has had primary responsibility for the Customer Risk Rating Methodology at a global bank, I do not see evidence of efforts by Blue Flame Medical to obfuscate the nature and purpose of the business. Indeed, given that Mr. Gula had been banking with Chain Bridge Bank for over 10 years, as well as the detailed discussion between Mr. Gula, Mr. Evinger, and Mr. Brough described below, I do not understand how Mr. Grice formed a belief that Blue Flame Medical was "reluctant" to provide information to Chain Bridge Bank, including about prior banking relationships, the names of its officers and directors, or its business location. In fact, Mr. Brough stated to Mr. Korpal the afternoon of March 26 that during his and Mr. Evinger's call the previous evening with Mr. Gula, "we asked him a number

[9] Grice Report ¶ 55.

of questions, he had all the answers to all the questions of course, but—and we thought—we didn't think anything was going to happen."[10]

Another indicator of suspicious activity on which Mr. Grice mistakenly relies is that "[t]he customer's background differs from that which would be expected on the basis of his or her business activities."[11] Based on my experience and review of the record, this indicator of suspicious activity was not present thanks to the March 25, 2020 phone call between Mr. Gula (on behalf of Blue Flame Medical) and Mr. Brough and Mr. Evinger (on behalf of Chain Bridge Bank). On that phone call, in addition to explaining the nature and purpose of Blue Flame Medical's business and the relevant details of the California transaction and the Wire Transfer, Mr. Gula openly discussed with Mr. Brough and Mr. Evinger that Blue Flame Medical marked a turning point in his career and life.[12] Mr. Gula said that he was excited to pursue a new career outside of politics and I am not aware of any indications that he attempted to deceive Mr. Brough and Mr. Evinger as to his experience in the medical supply industry. As with many of the indicators on Mr. Grice's list, this one typically raises Anti-Money Laundering concerns when the available information suggests the customer is trying to either achieve anonymity or create a false perception regarding their business or background. In my opinion, Mr. Gula—who fully disclosed his career shift and relative lack of experience in the PPE market prior to March 2020—was not attempting to do either.

Finally, Mr. Grice points to unfulfilled requests by Chain Bridge Bank for "copies of [Blue Flame Medical's] contracts" with its suppliers and the State of California as examples of another

[10] CBB00002541.
[11] Grice Report ¶ 55.
[12] *See* Gula Tr. 193-194.

indicator of suspicious activity listed in the FFIEC BSA/AML Manual: "[p]ayments or receipts with no apparent links to legitimate contracts, goods, or services . . . ."[13] That indicator of suspicious activity is intended to address payments that are unexplained or attempts (particularly in trade finance) to make transfers appear legitimate by copying or falsifying transaction documentation such as invoices, which, upon closer inspection, can be determined to be unrelated to the alleged underlying transaction.

In my opinion, this indicator of suspicious activity was not present in connection with the Wire Transfer because all facts learned by Chain Bridge Bank were consistent with the details of the transaction as initially explained to Chain Bridge Bank by Mr. Gula. The source and amount of the Wire Transfer matched the information that Mr. Gula had provided to Chain Bridge Bank on March 25. Further, California officials confirmed to Chain Bridge Bank shortly after it accepted the Wire Transfer that it was legitimate, authorized, and for the purpose that Blue Flame Medical had indicated—the purchase of 100 million N95 masks.[14] Once Chain Bridge Bank had received that confirmation directly from Blue Flame Medical's counterparty, the bank had no need for the document itself to confirm the payment was linked to a legitimate contract, goods, or services. Indeed, despite Chain Bridge Bank's claims that seeing the contract between Blue Flame Medical and the State of California was of great importance, it did not follow up on its request to Blue Flame Medical for that information or seek it from the California State Treasurer's Office on March 26 after placing a "hold" on the funds in Blue Flame

[13] Grice Report ¶ 55.
[14] CBB00002543; Brough Tr. 144-146.

Medical's account. In my experience, any doubt regarding the existence of the contract should have been resolved by the State of California's confirmation.[15]

ii. Blue Flame Medical provided advance notice to Chain Bridge Bank that it was expecting a larger wire amount than its disclosed anticipated activity.

Similar to the factor discussed above, Mr. Grice observes that the Wire Transfer was "substantially outside the disclosed and expected activity for Blue Flame Medical's account," and indicates that fact is "characteristic of potentially suspicious and concerning activity under BSA/AML regulations and industry practices."[16] While a difference in actual activity versus expected activity can raise red flags under certain circumstances, I do not believe those circumstances were present here due to the timing and nature of Blue Flame Medical's disclosures to Chain Bridge Bank.

As Mr. Grice notes, during the customer due diligence process at the time Blue Flame Medical opened its account, Mr. Gula indicated that the average total monthly wire transfer activity it expected to conduct would total approximately $125 million, with $100 million of that amount in the form of domestic wire transfers.[17] While I agree that the estimated average of expected wire activity Blue Flame Medical provided during the account opening process was significantly lower than the purchase price in the contract it entered into with the State of California later that day, it still represented very substantial monthly average wire activity, and

[15] I also disagree that any insistence by Chain Bridge Bank to vet Blue Flame Medical's contracts with its suppliers as a precondition to releasing the funds Chain Bridge Bank had credited to Blue Flame Medical's account would have been consistent with standard banking industry practice. *See* Grice Report ¶ 78. Such a request might have been reasonable in connection with transactional due diligence concerning outgoing wire transfers by Blue Flame Medical to those suppliers, but it is a step removed from the incoming wire to Blue Flame Medical from the State of California.

[16] *See* Grice Report at 45, ¶¶ 84-87.

[17] *See* Grice Report ¶ 26; Gula Tr. 143-144.

Blue Flame Medical notified Chain Bridge Bank of the anticipated size of the Wire Transfer the very same day, along with numerous other details regarding the transaction.[18] Furthermore, it does not appear that Chain Bridge Bank gave Blue Flame Medical any indication that the difference between the size of the Wire Transfer and the disclosed expected account activity would prevent it from accepting the transaction when Mr. Gula discussed the transaction with Mr. Brough and Mr. Evinger on March 25, or at any other point. Accordingly, I do not believe the estimate of expected average wire activity Blue Flame Medical included in its account opening information just hours before it notified Chain Bridge Bank of the size of the Wire Transfer indicated any reluctance by Blue Flame Medical to provide complete and accurate information to Chain Bridge Bank regarding its expected account activity.

Again, Mr. Grice attempts to justify Chain Bridge Bank's claims of concern regarding suspicious activity by quoting the FFIEC BSA/AML Manual's identification of circumstances where "[f]unds transfer activity is unexplained, repetitive, or shows unusual patterns."[19] None of those factors are present here. Mr. Gula explained the Wire Transfer to Chain Bridge Bank before it was sent, and the Wire Transfer was entirely consistent with that explanation, as was the subsequent confirmation of the amount, origination, and purpose of the Wire Transfer by the State of California. In light of Mr. Gula's disclosure and the corroborating information learned by Chain Bridge Bank, as well as the fact that Blue Flame Medical's account had just

[18] *See* CBB00002795.
[19] Grice Report ¶ 55.

been opened, the Wire Transfer did not constitute "repetitive" or "unusual pattern" activity. Indeed, the Wire Transfer was the first and only transaction in Blue Flame Medical's account.[20]

Finally, to the extent Mr. Grice intended to support his opinion by quoting the FFIEC BSA/AML Manual's example of suspicious activity including where a "[c]ustomer makes high-value transactions not commensurate with the customer's known incomes,"[21] that effort is misplaced and illustrates, in my opinion, his lack of understanding of actual Anti-Money Laundering practices. That quoted factor is inapplicable to these facts, since the concept of a customer making high-value transactions not commensurate with known incomes is only applicable in the context of consumer banking. That regulatory guidance is designed to address individuals, not corporations or business entities, and treats as suspicious any customer who is regularly making high-value transactions significantly in excess of their stated income, based on information provided in the customer due diligence process. Thus, it is inapplicable to a commercial business account like Blue Flame Medical's, particularly given Blue Flame Medical's disclosure as to the source and purpose of the funds sent in the Wire Transfer.

[20] Mr. Grice also states that the Wire Transfer reflected "unusual patterns" as part of his discussion regarding the lack of experience of both Blue Flame Medical and Chain Bridge Bank in processing wire transfers of this size. See Grice Report ¶ 87-92. In my experience, I do not believe either fact reflects a "pattern" relevant to Anti-Money Laundering concerns. In any event, based on my experience as an Anti-Money Laundering professional, I do not believe that Blue Flame Medical's lack of history receiving payments of this size is a sufficient basis within the banking industry to consider the transaction suspicious sufficient to return the funds following the acceptance of the Wire Transfer. Further, to the extent that Mr. Grice suggests that the fact that the Wire Transfer was 22 times larger than any that Chain Bridge Bank previously had handled, I do not believe that fact renders Blue Flame Medical's activity suspicious. If anything, it is a fact that Chain Bridge Bank should have disclosed to Blue Flame Medical on March 25 when it was informed of the transaction, if Chain Bridge Bank believed it relevant to its ability to process the Wire Transfer.

[21] Grice Report ¶ 55.

iii. None of Blue Flame Medical's alleged "unusual and suspicious behavior" justified Anti-Money Laundering concerns.

Mr. Grice's opinion that Blue Flame Medical's principals and employees exhibited unusual and suspicious behavior is factually baseless from an Anti-Money Laundering perspective.[22] The statement that it was unusual for Mr. Gula to come to the bank himself to open an account needs to be considered in context. I would consider it reasonable for anyone who wanted an account opened the same day to go to the bank to see that the process is completed. In-person customer account applications are actually considered less concerning from an Anti-Money Laundering perspective because in-person interactions do not permit the same level of anonymity that is possible through online or electronic customer account applications.

Blue Flame Medical's statements to Chain Bridge Bank regarding the urgency of its need to know when the funds had been received from the State of California or to send outgoing wires to the suppliers for the masks purchased by the State of California did not constitute an "unexplained urgency to transfer funds" within the meaning of Anti-Money Laundering guidance.[23] Both Mr. Gula and Mr. Thomas explained Blue Flame Medical's need for that information to Chain Bridge Bank representatives—to confirm with its suppliers that it would be sending payment for scarce PPE in high demand to its suppliers as quickly as possible.[24]

Another indicator of suspicious activity erroneously cited by Mr. Grice related to this concept of "unusual and suspicious behavior" is when a "[c]ustomer has established multiple accounts in various corporate or individual names that lack sufficient business purpose for the

[22] *See* Grice Report ¶¶ 93-97.
[23] *See* Grice Report ¶¶ 95-97.
[24] *See* CBB00002786; CBB00002795.

account complexities or appear to be an effort to hide the beneficial ownership from the bank."[25] But no such facts are present here. This indicator concerns instances where a business establishes multiple accounts, often without the appearance of legitimate purpose, that can be used to move money back and forth between accounts—possibly exploiting false invoicing or other money laundering techniques to help conceal the true origin of the funds. The accounts opened by Mr. Gula in March 2020 for three different business organizations[26] do not, in my opinion, fit this pattern, nor am I aware of any facts suggesting that Blue Flame Medical attempted or intended to transfer funds to or from any of those other accounts. To suggest that the purpose of the accounts was to hide beneficial ownership would be nonsensical under the circumstances. Mr. Gula had been a customer of Chain Bridge Bank for over 10 years, was one of two beneficial owners of Blue Flame Medical, and evidently had provided information on Blue Flame's other owner—John Thomas, for whom Chain Bridge Bank would have recently conducted customer due diligence in connection with the opening of other accounts—adequate to satisfy Chain Bridge Bank's customer due diligence requirements in opening the Blue Flame Medical account.

iv. Neither the Wire Transfer nor Blue Flame Medical's anticipated business activity presented concerns regarding "high velocity transactions" from an Anti-Money Laundering perspective.

Mr. Grice's opinion that the Wire Transfer was a "'high velocity' transaction"[27] exaggerates the relevant facts and is meritless. First of all, the regulatory concept that Mr. Grice is referencing concerning a "high velocity" of funds flow concerns a bank's monitoring of

---

[25] *See* Grice Report ¶ 55.
[26] *See* Grice Report ¶¶ 23-25.
[27] *See* Grice Report ¶¶ 98-99.

transactions in a customer's account over a specific period of time, not individual transactions.[28] "High velocity" accounts are, by definition, accounts with significant amounts of deposits and withdrawals, often by electronic means, reflecting a "high velocity" of funds movement through the account. In Anti-Money Laundering, the primary concern with respect to "high velocity" accounts is that they are commonly used as "funnel accounts." A "funnel account" is an account that is opened with a small balance, and then left dormant for several weeks, often months, followed by a large (often overseas) wire transfer sent to the account, only to have those funds immediately wired off to other accounts – thus, the "high velocity." This technique is used in the "layering" stage of money laundering, and is part of an effort to obscure the true source of the funds.

Blue Flame Medical's account did not fit the profile of a "high velocity" account, nor did the Wire Transfer from the State of California to Chain Bridge Bank implicate the Anti-Money Laundering concerns associated with such accounts. Given that the Wire Transfer was the first transaction for Blue Flame Medical's account, it is impossible to consider the account as "high velocity" as no such pattern of transactional activity had been established.

Furthermore, Mr. Grice misrepresents and exaggerates the evidence regarding Blue Flame Medical's plans and its communication of those plans in his report where he says that "Mr. Gula insisted that any funds received would need to be wired out immediately."[29] While Blue Flame Medical told Chain Bridge Bank that it would need to be able to quickly pay its

---

[28] *See* Grice Report ¶ 99; "Appendix O: Examiner Tools for Transaction Testing," FFIEC BSA/AML Manual, 2014, p.O-3, available at: https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed March 11, 2021.
[29] Grice Report ¶ 79.

suppliers to secure N95 masks for California's order, and Mr. Gula informed Chain Bridge Bank on March 25 that Blue Flame Medical intended to send outgoing wires from its account for that reason, he made clear that not all of the funds would be wired out (because Blue Flame Medical's profit would be retained in the account), and that the funds would be paid out as the masks were manufactured, and "not … all at once."[30] Mr. Gula further informed Chain Bridge Bank that he would provide more detail to the bank on March 26 concerning the timing of those anticipated outgoing wires.[31] I am not aware of any such information being discussed between Mr. Gula and Chain Bridge Bank personnel on March 26, and note that Chain Bridge Bank personnel were ordered that day not to speak to Mr. Gula by Mr. Evinger and Mr. Brough.[32]

v. Neither the Wire Transfer nor Blue Flame Medical's anticipated business activity involved "high-risk jurisdictions."

Mr. Grice's suggestion that that the Wire Transfer between the State of California and Chain Bridge Bank involved a "high-risk jurisdiction"[33] simply ignores the facts. The Wire Transfer involved exclusively domestic entities and accounts, including the State of California's account at JPMorgan Chase, an extremely sophisticated United States financial institution. As an Anti-Money Laundering professional who has been responsible for the Anti-Money Laundering risk ratings of all jurisdictions around the world for two global banks during my career, I know from first-hand experience that no financial institution considers California, Virginia, or the United States to be high-risk jurisdictions.

---

[30] CBB00002795.
[31] CBB00002795.
[32] *See* CBB00002795; CBB00000748; CBB00000919; CBB00000661.
[33] Grice Report ¶¶ 100-101.

Mr. Grice appears to base his opinion regarding the involvement of high-risk jurisdictions on the payments Blue Flame Medical planned to make to its suppliers for the California order.[34] However, none of those planned wire transfers would have involved "high-risk jurisdictions" either. As Mr. Grice recognizes, Mr. Gula informed Chain Bridge Bank that all of its anticipated outgoing wires to its suppliers would be sent to United States entities with accounts at United States-based financial institutions.[35] As a result, Chain Bridge Bank could and would have reasonably been able to have "reliance," based on the regulatory definition of the term, on each of those financial institutions' compliance with Anti-Money Laundering regulations in connection with each and every one of Blue Flame Medical's planned outgoing wires in connection with its contract with the State of California, as the United States' Anti-Money Laundering regulatory regime expressly permits such reasonable reliance.[36] Thus, while the transfers Blue Flame Medical intended to make to its suppliers did concern the purchase of products manufactured in China—which is extremely common in commercial purchase transactions—no transfers to China would have been made by Blue Flame Medical or from its account at Chain Bridge Bank. To the extent Mr. Grice's opinion is based on the possibility that funds would eventually be sent offshore to a "high-risk jurisdiction," any such transfer would not have been made by Blue Flame Medical or involve Chain Bridge Bank, and in any event would have been a subsequent transfer subject to at least one additional layer of transactional due diligence by established United States financial institutions. Accordingly, Blue Flame

[34] *See* Grice Report ¶ 100.
[35] *See* Gula Tr. 191; BFM000013445.
[36] *See* 31 CFR 1020.220

Medical's anticipated outgoing wires to its suppliers are irrelevant from an Anti-Money Laundering assessment of the Wire Transfer.

vi. JPMorgan Chase's "concerns of fraud" did not appear to impact Chain Bridge Bank's actions.

Mr. Grice's opinion that JPMorgan Chase had "concerns of fraud" is reasonable, based upon the record, and would have supported Chain Bridge Bank's actions in placing a "hold" on the funds in Blue Flame Medical's account to conduct further diligence.[37] However, I note that Chain Bridge Bank had already placed a "hold" on the funds at the time JPMorgan Chase contacted Chain Bridge Bank and expressed that opinion, so it does not appear to have had any impact on Chain Bridge Bank's diligence process.[38] More fundamentally, based on my review of the record, it does not appear that Chain Bridge Bank discovered any additional information regarding Blue Flame Medical based on any investigation related to JPMorgan Chase's communicated concerns.

B. Response to Grice Opinion No. 2

I disagree with Mr. Grice's opinion that the actions taken by Chain Bridge Bank after it opened Blue Flame Medical's account and accepted the Wire Transfer on behalf of Blue Flame Medical were reasonable and consistent with industry standards and practices. Mr. Grice bases his opinion on the following:

a. His belief that Chain Bridge Bank's actions in contacting the State of California to ask questions about the Wire Transfer and reveal information about its customer, asking JPMorgan Chase to request a recall of the Wire Transfer, and closing Blue Flame's account were all reasonable and consistent with industry standards and practices;[39] and

[37] Grice Report ¶ 102.
[38] *See* Coffey Tr. at 64-65; CBB00004468.
[39] *See* Grice Report ¶ 104.

b. His evident belief that Chain Bridge Bank could not simultaneously comply with all applicable banking laws and regulations while conducting due diligence and resolving any concerns regarding potentially suspicious activity.[40]

Based upon my experience and review of documents in this litigation, I believe Chain Bridge Bank's actions—particularly its contacts with the State of California and JPMorgan Chase concerning the Wire Transfer—were highly unusual and deviated from standard banking industry standards and practices. Furthermore, I believe that if Chain Bridge Bank wished to simultaneously comply with Regulation J and meet all applicable obligations to investigate and report suspicious activity, it could have done so.

i. Chain Bridge Bank's actions in contacting the State of California, requesting that JPMorgan Chase issue a recall of the funds, and agreeing to return those funds violated industry standards and practices and applicable regulations.

Mr. Grice states three key opinions in his report concerning Chain Bridge Bank's contacts with the State of California and its bank, JPMorgan Chase, which I believe are incorrect, inaccurate, or misleading.

First, Mr. Grice opines that a bank communicating with a non-customer regarding a transaction, as Chain Bridge Bank did regarding Blue Flame Medical with the State of California, was "reasonable and consistent with industry standards and practices."[41] Based on my experience as an Anti-Money Laundering professional, that is not true. If acting on behalf of a *sending* bank in connection with a wire transfer, it may be consistent with standard practice to contact the receiving bank and/or its customer if questions arise concerning the transfer. However, I have never heard of a *receiving* bank contacting a non-customer to raise questions

[40] *See* Grice Report ¶ 105.
[41] *See* Grice Report ¶ 104.

regarding an incoming wire transfer prior to my engagement in this action. I have even asked this question of a number of my Anti-Money Laundering peers in the banking industry and none could recall a single instance of contacting a non-customer regarding a wire transfer when their institution was the receiving bank, like Chain Bridge Bank was in this instance.

Putting aside how unusual the act of contacting a non-customer regarding an incoming wire transfer is in the first place, it might be somewhat understandable if Chain Bridge Bank did so in order to confirm the details of the wire transfer with the State of California. But it does not appear that was Chain Bridge Bank's intent. Indeed, even after Fee Chang of California's Department of General Services confirmed the amount of the wire transfer and the fact that Blue Flame Medical was the intended beneficiary, Chain Bridge Bank asked to speak to the State Treasurer's Office—despite the fact that the payment order Chain Bridge Bank received indicated that the Wire Transfer had been made "BY ORDER OF DEPARTMENT OF GENERAL SERVICES."[42] Then, during the call it requested with the State Treasurer's Office, Chain Bridge Bank disclosed information about Blue Flame Medical without Blue Flame's permission.[43] In my entire 30+-year career in financial services, I have never heard of a bank calling a non-customer to provide information to the non-customer about the bank's customer. In my opinion, to represent such an action as "consistent with industry standards and practices" is entirely inaccurate. To the extent Mr. Grice bases his opinion concerning such actions on Section 314(b) of the USA PATRIOT Act,[44] that law only concerns sharing of information between financial institutions, not a financial institution and a non-financial institution, non-customer of a bank.

[42] CBB00002543; CBB00002649.
[43] *See* Brough Tr. at 278-282.
[44] *See* Grice Report ¶ 59.

Second, Mr. Grice opines that Chain Bridge Bank's actions in "honoring JPMorgan's request to return the California Wire Transfer" were consistent with industry standards and practices.[45] To represent Chain Bridge Bank's actions surrounding the return of the funds to JPMorgan Chase as merely "honoring JPMorgan Chase's request to return the wire transfer"[46] is a gross distortion of the facts because it ignores that Chain Bridge Bank asked JPMorgan Chase to request that the funds be returned.[47] As I noted in my Initial Report, JPMorgan Chase initially responded that it would not request a recall of the funds and that it was comfortable with Chain Bridge Bank "holding" the funds.[48] Indeed, Mr. Korpal testified that he decided to make the recall request on behalf of JPMorgan Chase in response to Chain Bridge Bank's request that it do so.[49] It is not consistent with industry standards and practices for a beneficiary's bank to ask the originator's bank to request a return of funds intentionally sent to its customer, or attempt to cancel a wire transfer that had already been accepted.[50]

Third, Mr. Grice opines that closing "Blue Flame Medical-related accounts" was reasonable and consistent with industry practice.[51] As an Anti-Money Laundering professional

[45] *See* Grice Report ¶ 104.
[46] Grice Report ¶ 12; *see also* Grice Report ¶ 104.
[47] *See* Korpal Tr. at 23, 79, 248-250.
[48] *See* CBB00002544; Korpal Tr. 250.
[49] *See* Korpal Tr. 250-51.
[50] To the extent Mr. Grice opines in the Grice Report (or his other, 11-page report) that Chain Bridge Bank returned the funds to JPMorgan Chase by "canceling" the Wire Transfer (*see* Grice Report ¶ 50), he is mistaken based on my experience and understanding of the relevant regulations. Once Chain Bridge Bank accepted the Wire Transfer and credited Blue Flame Medical's account, the transfer was complete and final. That is consistent with the statement in Section 211(c) of Regulation J/Article 4A that an accepted payment order may only be canceled in the limited "fat finger" circumstances described below. *See* Uniform Commercial Code, § 4A-211(c)(2), cmts. 1, 3, 4. The subsequent transfer of funds in response to the recall notice that JPMorgan Chase issued at Chain Bridge Bank's request was a new, separate transfer requiring a new payment order as that term is defined in Section 103(a)(1) of Regulation J/Article 4A, which Chain Bridge Bank sent on behalf of Blue Flame Medical as originator without Blue Flame Medical's consent or approval. *See* Uniform Commercial Code, § 4A-103(a)(1); CBB00002653.
[51] Grice Report ¶ 104.

who has been the primary owner of the Customer Risk Rating Methodology and Risk Appetite Statement at a global bank, I am aware that banks can close a customer account for a variety of reasons, one of those being that the account is outside of the bank's risk appetite. However, it is bizarre that Chain Bridge Bank allowed the account to remain open and accepted the Wire Transfer despite being told in advance about the transaction's size (which was 22 times larger than anything processed by Chain Bridge Bank previously) and essential terms,[52] only to change its mind after the Wire Transfer actually materialized. Indeed, despite being told in detail the night before the Wire Transfer that it would be made and having been provided a copy of correspondence between a representative of California's Department of General Services and Blue Flame Medical stating that the wire would be processed the morning of March 26,[53] Mr. Brough's immediate reaction to learning the Wire Transfer had been received was to state, "Unbelievable. We are going to try to contact the sender."[54]

Chain Bridge Bank's decision to close Blue Flame Medical's account and other accounts opened by Mr. Gula also does not appear to have been driven by applicable regulations or its policies and procedures concerning suspicious activity reporting. As recently stated in a joint release by the federal banking agencies, a bank is not required to close a customer account even after identifying suspicious activity and filing a SAR. [55] Similarly, Chain Bridge Bank's "Suspicious Activity Procedures" policy provides that customers "who are the subject of

---

[52] *See* Brough Tr. 131-134, 351.
[53] *See* Brough Tr. 131-134; CBB00002699-2700.
[54] CBB00002725.
[55] *See* Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, "Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations," at 3 (January 19, 2021), *available at* https://www.fincen.gov/sites/default/files/2021-01/Joint%20SAR%20FAQs%20Final%20508.pdf, accessed March 11, 2021.

multiple SAR filings will be reviewed for account closure" and will be "classified as high risk and will be monitored closely for further activity unless the activity is considered illegal or unless a loss occurs, in which cases the accounts will be closed."[56] Although Chain Bridge Bank's BSA Officer and CEO retained the discretion to make determinations regarding account closure "in other cases based on the severity of the suspicious activity and its duration,"[57] it does not appear from my review of the record that Chain Bridge Bank ever determined that any action by Blue Flame Medical was illegal or caused a loss for Chain Bridge Bank.

ii. Chain Bridge Bank could have conducted appropriate and industry-standard due diligence without requesting to return the funds to JPMorgan Chase or returning a completed wire transfer in violation of Regulation J.

Mr. Grice's report suggests that Blue Flame Medical's interpretation of Regulation J in this litigation means that a bank that has received and accepted a wire transfer on behalf of a customer must either abstain from conducting due diligence if presented with suspicious activity or process transactions and make the funds available to the customer without conducting appropriate diligence.[58] That is untrue and presents a false choice, as it overlooks several available options (some of which were employed by Chain Bridge Bank before it abruptly asked JPMorgan Chase to recall the funds Chain Bridge Bank had credited to Blue Flame Medical's account) to achieve all regulatory compliance objectives. Based on my extensive experience with various regulatory authorities, I know that every regulator expects financial institutions to comply with *all* regulatory requirements, not just some of them.

---

[56] CBB00004274 at 4275-76.
[57] CBB00004274 at 4276.
[58] *See* Grice Report ¶ 105.

In the instance of the Wire Transfer from the State of California to Blue Flame Medical, Chain Bridge Bank put a "hold" on the funds after they were credited to the account of Blue Flame Medical.[59] Based on the screenshots of the activity in the account of Blue Flame Medical on March 26, 2020, the funds were credited shortly after noon and Chain Bridge Bank put a "hold" on the funds in Blue Flame Medical's account shortly thereafter.[60] That action—putting a 'hold' on funds when there are concerns of potentially suspicious activity—is reasonable and consistent with industry standards, since it allows the bank to keep control of the funds while continuing to conduct due diligence. Even after Chain Bridge Bank confirmed with the State of California that Blue Flame Medical was entitled to the funds, it kept the "hold" in place to continue to block Blue Flame Medical's access to the funds. Doing so was consistent with JPMorgan Chase's desire that Chain Bridge Bank put a "hold" on the account while they continue to conduct additional due diligence on the transaction,[61] and in my opinion was consistent with applicable Anti-Money Laundering regulations.

What Chain Bridge Bank did after that, however, violated applicable regulations and standard industry practice. In discussing the Wire Transfer with JPMorgan Chase, Chain Bridge Bank represented to JPMorgan Chase that it had not credited Blue Flame Medical's account with the funds,[62] even though Chain Bridge Bank personnel internally discussed the fact that the bank had credited those funds to Blue Flame Medical's account.[63] Chain Bridge Bank then requested that JPMorgan Chase issue a recall for the Wire Transfer, to which JPMorgan Chase

[59] CBB00004468; *see also* CBB00002673; CBB00002649; CBB00000971 at 973.
[60] CBB00002673; CBB00004468.
[61] *See* Korpal Tr. at 231-32; Coffey Tr. 68-69.
[62] *See* Korpal Tr. at 62-63, 72, 139, 142-43, 232.
[63] *See* CBB00002649; CBB00000971 at 973; CBB00002789.

complied even though it did not plan to do so but for Chain Bridge Bank's request.[64] Putting the apparent misrepresentation by Chain Bridge Bank and the irregularity of its request to the side, I am not aware of any facts suggesting that Chain Bridge Bank had discovered through any due diligence that Blue Flame Medical was not entitled to the funds wired for its benefit by the State of California at the time it made that request. As a result, it does not appear that Chain Bridge Bank's investigations into potential suspicious activity had reached any conclusions at the time it requested that JPMorgan Chase recall the Wire Transfer or at the time it returned the funds. Indeed, apart from obtaining confirmation that the State of California did intentionally send the Wire Transfer to Blue Flame Medical for the reason Blue Flame Medical described, it does not appear that Chain Bridge Bank pursued any other information regarding the transaction from either the State of California or JPMorgan Chase.[65] Rather than ensure compliance with the regulatory requirements, I believe that those actions by Chain Bridge Bank violated Regulation J.

Regulation J (section 4A-404) states that the beneficiary bank, upon accepting a payment order, is obligated to pay the amount of the order to the beneficiary—unless the bank proves that it did not pay because of a reasonable doubt concerning the right of the beneficiary

[64] Korpal Tr. at 23, 79, 248-250.

[65] I am aware that there is a partially recorded phone conversation between Mr. Evinger and Fee Chang of the State of California Department of General Services on March 26, 2020 in which Mr. Evinger seems to state, in response to Ms. Chang's statement that the Wire Transfer "is a good transfer," that "it would be helpful, if there is documentation to support it." CBB00002543. However, after Ms. Chang responded that the transfer was made by the State of California State Treasurer's Office, Ms. Chang asked, "do you need any information from us, or you need to reach out to our State Treasurer's Office," Mr. Evinger responded only that it would be helpful to speak to the State Treasurer's Office. I am not aware of any requests made by Chain Bridge Bank to the State Treasurer's Office for any additional information or documentation concerning the transaction, nor am I aware of any follow-up requests by Chain Bridge Bank to the Department of General Services (or Blue Flame Medical) for more information or documentation after Chain Bridge Bank placed the "hold" on the funds in Blue Flame Medical's account on March 26.

to payment.[66] Based on my experience, this provision in Regulation J is typically used when the payment order contains an error regarding the beneficiary's account information. Indeed, such an error is expressly identified elsewhere in Regulation J as one of the limited circumstances in which a bank can agree to cancel an accepted payment order.[67] Errors regarding the beneficiary's account information include an incorrect beneficiary name, an incorrect account number, an incorrect beneficiary bank, and other so-called "fat fingered errors." Similarly, the official comments to Section 404 further reinforce that the concept of "reasonable doubt" does not include claims that the beneficiary of the wire procured the funds through fraud.[68] Since Chain Bridge Bank knew that the payment order did not contain an error regarding the beneficiary's account information and knew the payment was intended for Blue Flame Medical, I am not aware of any basis Chain Bridge Bank would have had to refuse to make payment to Blue Flame Medical under Regulation J.

Similarly, Chain Bridge Bank's Wire Transfer Policy does not appear to provide any basis for the bank's decision to return the funds sent by the State of California to Blue Flame Medical. The "Incoming Wires" section of the policy states only that the bank reserves the right to return incoming wires "[i]f the Bank notices a discrepancy between the beneficiary account number and beneficiary name" or "if there is any question as to the beneficiary's right to the funds, such as a discrepancy between name and account number…"[69] Again, there was no discrepancy regarding the account name or number for Blue Flame Medical in connection with

[66] *See* Uniform Commercial Code, § 4A-404(a).
[67] *See* Uniform Commercial Code, § 4A-211(c)(2).
[68] *See* Uniform Commercial Code, § 4A-404(a), cmt. 3.
[69] CBB00004294 at 4298.

the Wire Transfer, and any question as to Blue Flame Medical's right to the funds should have been eliminated at the time the State of California confirmed the wire was sent to Blue Flame Medical in the amount and for the purpose that Blue Flame Medical had represented to Chain Bridge Bank.

Mr. Grice attempts to justify those actions and any violations of Regulation J by claiming that Chain Bridge Bank's raising of concerns was compliant with BSA/AML Regulations.[70] But Chain Bridge Bank does not have to choose between complying with Regulation J and raising concerns or investigating activity it believes is suspicious. Chain Bridge Bank could have maintained the "hold" on the account until the following day consistent with Anti-Money Laundering regulations and permitting the investigation into potentially suspicious activity to be resolved. Although Chain Bridge Bank would have had to release that "hold" the next day, it could have placed a "freeze" on Blue Flame Medical's account (as provided in the terms of the account agreement)[71] and continued investigating potential suspicious activity if necessary. Chain Bridge Bank also would have additional diligence opportunities in connection with subsequent outgoing wire transfer requests by Blue Flame Medical. Similarly, nothing in Regulation J, the BSA, nor Chain Bridge Bank's policies and procedures prohibited it from filing a SAR in response to suspicious activity or required it to refuse to make the funds available (or send the funds back after accepting the payment order on behalf of Blue Flame Medical) due to a SAR being filed.

---

[70] *See* Grice Report ¶¶ 62-63.
[71] *See* CBB00002765 at 2769

Thus, even if Chain Bridge Bank had continued to investigate the transaction, and even if it had confirmed the transaction was suspicious, that does not mean Chain Bridge Bank was forced to choose between violating Regulation J and other potentially applicable regulations. Indeed, Chain Bridge Bank was free to reject any request to return the funds under Regulation J from JPMorgan Chase while continuing to exercise other options available under the BSA and other applicable regulations to investigate and report suspicious activity. Consistent with the opinions stated in my Initial Report, the fact that Chain Bridge Bank did not pursue those options and instead took the highly unusual step of asking JPMorgan Chase to issue a recall request suggests it was more concerned about recognizing the deposit on its balance sheet than it was in completing an appropriate investigation consistent with standard industry practices.[72]

Furthermore, Mr. Grice's opinion appears to ignore Chain Bridge Bank's obligations not to accept unauthorized payment orders for its customers' accounts under Section 204 of Regulation J. This regulation states that if a receiving bank accepts a payment order issued in the name of its customer as sender, which is not authorized and not effective as the order of the customer, or not enforceable, in whole or in part, against the customer, the bank shall refund any payment of the payment received from the customer.[73] This means that if the receiving bank sends a payment out of a customer account that was not authorized or provided by the customer, or not enforceable, the bank has to refund the payment to the customer.

[72] *See* Initial Report at 14-15.
[73] *See* Uniform Commercial Code, § 4A-204(a).

Here, Chain Bridge Bank accepted the wire transfer from the State of California on behalf of its customer, Blue Flame Medical. Chain Bridge Bank claims it regarded the transaction as potentially suspicious and, rather than waiting for the investigation to reach a conclusion, agreed to send a payment out of their customer's account that was neither provided by nor authorized by the customer, and has not refunded the payment to the customer. As an Anti-Money Laundering professional, I know that it is a violation of applicable regulations to initiate a transaction from a customer's account without their permission unless I have legal and/or regulatory authorization to do so. I am not aware of any legal or regulatory authorization for such action in this case, and have never heard of an institution initiating a transaction out of a customer account absent *both* customer approval *and* legal or regulatory authorization to do so.

This report summarizes my opinions to date regarding the Grice Report. If additional information is produced between now and trial, I reserve the right to supplement my report.

Signed:

Sean O'Malley

APPENDIX A

Materials considered in connection with Initial Report:

Pleadings and Court Papers

Complaint, *Blue Flame Medical LLC v. Chain Bridge Bank, N.A., et al.*, Case No. 20 Civ. 658 (June 12, 2020)

Third-Party Complaint, *Blue Flame Medical LLC v. Chain Bridge Bank, N.A., et al.*, Case No. 20 Civ. 658 (Oct. 13, 2020), and exhibits thereto

Answer and Defenses of JPMorgan Chase Bank, N.A. to Chain Bridge Bank, N.A.'s Third-Party Complaint, *Blue Flame Medical LLC v. Chain Bridge Bank, N.A., et al.*, Case No. 20 Civ. 658 (Nov. 16, 2020)

Deposition Transcripts

Deposition of Mike Gula, January 12, 2021

Deposition of David Evinger, January 29, 2021

Deposition of John Brough, February 2, 2021

Deposition of Rakesh Korpal, February 9, 2021 ("Realtime")

Deposition of Tim Coffey, February 12, 2021 ("Realtime")

Audio Recordings Produced in Litigation

CBB00000707

CBB00002541

CBB00002543

CBB00002544

CBB00002545

CBB00002789

CBB00002794

CBB00002795

CBB00002797

CBB00002798

Documents Produced in Litigation (Beginning Bates Number)

BFM000013445

BFM000074101

CBB00000527

CBB00000594

CBB00000640

CBB00000643

CBB00000655

CBB00000661

CBB00000718

CBB00000741

CBB00000748

CBB00000761

CBB00000779

CBB00000795

CBB00000807

CBB00000815

CBB00000818

CBB00000853

CBB00000919

CBB00000971

CBB00001008

CBB00001097

CBB00001202

CBB00001385

CBB00001514

CBB00001725

CBB00001770

CBB00001781

CBB00001938

CBB00001939

CBB00002529

CBB00002563

CBB00002655

CBB00002649

CBB00002650

CBBB0002653

CBB00002661

CBB00002673

CBB00002699

CBB00002725

CBB00002779

CBB00002780

CBB00002781

CBB00003573

CBB00004294

CBB00004307

CBB00004323

CBB00004442

CBB00004445

CBB00004446

Regulations, Statutes, Manuals, and Advisories

Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA) / Anti-Money Laundering (AML) Examination Manual

Financial Crimes Enforcement Network (FinCEN) Advisories related to COVID-19

Customer Due Diligence guidelines from the Federal Financial Institutions Examination Council (FFIEC)

Federal Reserve Bank Regulation P

Uniform Commercial Code 4A-404(a) and 4A-211(c)

Federal Reserve Bank Maintenance Manual, November 2019

Additional Materials Considered in Connection with Rebuttal Report:

Deposition Transcripts

Deposition of Claudia Mojica-Guadron, January 26, 2021

Deposition of Heather Schoeppe, January 22, 2021

Documents Produced in Litigation (Beginning Bates Number)

CBB00002786

CBB00004468

CBB00004274

CBB00002765

CBB00004277

CBB00004325

CBB00004279

CBB0004302

CBB0004310

CBB000200751

Regulations, Statutes, Manuals, and Advisories

31 CFR § 1020.220 - Customer identification program requirements for banks.

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, "Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations".

Opposing Party Expert Reports

Expert Report of Charles H. Grice, February 12, 2021[74]

Expert Report of Charles H. Grice, February 12, 2021[75]

Expert Report of Teresa Pesce, February 12, 2021

[74] Mr. Grice issued two identically titled reports dated February 12, 2021; one is 59 pages in length and the other is 11 pages. This reference is in regard to the 59-page report issued by Mr. Grice.
[75] Mr. Grice issued two identically titled reports dated February 12, 2021; one is 59 pages in length and the other is 11 pages. This reference is in regard to the 11-page report issued by Mr. Grice.