EXHIBIT 53

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

EXPERT REPORT OF CHARLES H. GRICE
February 12, 2021

TABLE OF CONTENTS

I. QUALIFICATIONS

1. I am the co-founder and Managing Director and Principal of CRI Compliance ("CRI"), a company dedicated to developing compliance and risk management programs for financial institutions. I have over 30 years of experience within the banking industry working as a consultant with financial institutions on regulatory and risk management matters. Much of this work has been performed under the supervision of federal and state banking regulators or has involved consulting to federal and state banking regulators. I previously served as the Assistant Director of the California Bankers Association ("CBA"), as a Research Assistant for the Federal Reserve Board ("FRB"), and as a Legislative Analyst for U.S. Senator Lloyd Bentsen for the U.S. Senate's Committee on Housing, Banking, and Urban Affairs.

2. Following professional positions with the U.S. Senate, FRB, and CBA, I co-founded CRI in 1988. Since then, I have provided risk management and compliance consulting to banks and have consulted for governmental agencies. My consulting work has involved hundreds of clients throughout the United States and abroad. My work includes the design and testing of compliance and risk management programs, analysis of specific transactions based on industry standards and practices, development and performance of risk assessments, testing or evaluation of compliance systems, and analysis related to government investigations.

3. My specific areas of expertise include industry standards and practices to comply with Bank Secrecy Act/anti-money laundering ("BSA/AML") regulations, laws and regulations pertaining to account opening, funds transfer, and transaction monitoring (e.g., the USA PATRIOT Act and the FRB's Regulation J), and other risk management requirements relevant to national banks. I am routinely hired to advise banks on their regulatory compliance programs, including the design and evaluation of compliance programs related to suspicious transactions that implicate

risks of fraud, money laundering, and avoidance of government sanctions programs (e.g., the Office of Foreign Assets Control ("OFAC")). This work involves evaluating, and at times managing, compliance officers and staff; reviewing, testing, and modifying compliance software; assessing audit programs; and developing and evaluating policies and procedures. The vast majority of my consulting assignments have included a focus on financial institutions' systems for conducting funds transfers and transaction monitoring. My clients have included four of the five largest banks in the United States, as well as dozens of international banks. My work is regularly evaluated by federal and state bank examiners, including the Office of the Comptroller of the Currency ("OCC"), FRB, and the Federal Deposit Insurance Corporation ("FDIC"), as well as U.S. law enforcement.

4. Since 1994, I have worked as a board-appointed Compliance Officer for several U.S. banks on an interim project basis, ranging from a few months to several years. These engagements are specifically focused on responding to regulatory criticisms of the subject banks' BSA/AML and other regulatory compliance programs. Frequently, these regulatory criticisms consist of enforcement actions or other criticisms from a bank's regulators and/or auditors relating to its funds transfer and transaction monitoring practices. In these positions, I have provided guidance to officers and staff, made decisions on accounts and transactions, counseled the Board of Directors and executive management, and worked with auditors and state and federal bank examiners. Between 2006 and 2009, I served as chief compliance and/or chief risk officer for six banks on assignments that lasted from six to 36 months. In addition, I have served as a consultant to over 100 banks, implementing BSA/AML and other regulatory compliance procedures.

5. I have been recognized by numerous governmental entities as an expert in banking industry standards and practices relating to regulatory compliance and internal controls, including

BSA/AML compliance. I have testified before the U.S. Senate Banking Committee, the OCC, the FRB, the FDIC, and the California State Legislature, among others. I have briefed and presented seminars for law enforcement officials and bank examiners on funds transfer and transaction monitoring, including the Department of Justice, Federal Bureau of Investigation ("FBI"), Financial Crimes Enforcement Network ("FinCEN"), Internal Revenue Service, state regulators, the State Department's Bureau of Counterterrorism, and the Large Bank Examination Division of the OCC. I have participated as a U.S. national delegate with the U.S. Treasury Department's Public-Private Dialogue in São Paulo, Brazil, and at similar fora in Bishkek, Buenos Aires, London, Madrid, Mexico City, Moscow, Seoul, Singapore, and Tokyo. I have provided technical assistance on internal banking controls to the central banks of Kyrgyzstan, Russia (CIS), South Korea, Spain, Taiwan, Tanzania and Tunisia as part of projects funded by the U.S. Department of the Treasury and the State Department's Bureau of Counterterrorism. Recently, I completed a three-year assignment on a project for a global financial institution that was mandated and overseen by state and federal agencies. This work required a detailed knowledge of legal and regulatory requirements and banking industry practices relating to funds transfer and transaction monitoring, and included hundreds of hours of meetings with state and federal law enforcement and supervisory agencies, internal and external audit teams, and senior bank executives, each working to modernize payment platforms.

6. I have delivered hundreds of compliance seminars to banks, regulators (e.g., the OCC and California Banking Department), national trade associations (e.g., American Bankers Association, American Bar Association, Consumer Bankers Association, and Risk Management Association), state trade associations, and international bankers. Outside the United States, I have advised foreign governments and spoken at over 50 international risk management and compliance

conferences. I have trained thousands of banking professionals on BSA/AML and other regulations, including officials from the U.S. Department of Treasury and the OCC, and have presented before national meetings of the American Bar Association, the American Bankers Association, and dozens of other national and international banking groups including national trade associations (e.g., Association of Certified Anti-Money Laundering Specialists, Bank Administration Institute, Caribbean Anti-Money Laundering Conference, Consumer Bankers Association, Risk Management Association, U.S. League of Savings Institutions, West Coast Anti-Money Laundering Forum, and Western Independent Bankers), and state trade associations (e.g., CBA, Connecticut Bankers Association, Florida International Bankers Association, Hawaii Bankers Association, Illinois Bankers Association, Massachusetts Bankers Association, New Jersey Bankers Association, New Jersey Mortgage Bankers Association, and Puerto Rico Bankers Association).

7. I received a Bachelor of Arts degree from the Johns Hopkins University in 1980 and a Master's degree in Public Policy from the Kennedy School of Government at Harvard University in 1985. I completed additional graduate training in economics at The George Washington University, the Johns Hopkins School of Advanced International Studies, and the Getulio Vargas Foundation in Rio de Janeiro, Brazil, where I was a Fulbright Scholar. I have benefitted from several highly selective fellowships including a Fulbright Fellowship, an International Telephone & Telegraph Fellowship, and a three-year W.K. Kellogg National Fellowship.

8. I have performed analyses of banks and other financial institutions' practices regarding BSA/AML and other regulatory compliance in a wide variety of litigation matters since 1999. I have either testified or consulted in more than 25 matters involving allegations of improper,

unauthorized, or fraudulent funds transfers, including those related to money laundering, tax evasion, and identity theft. I have also consulted on BSA/AML and other regulatory compliance matters for the United States Department of Justice, state governments, the President and Minister of Justice for Chile (regarding the banking transactions of former president Augusto Pinochet), and several foreign central banks and ministries of finance. I have been qualified and have testified as an expert on regulatory compliance and banking matters in multiple state and federal courts throughout the United States, including in California, Florida, Georgia, New York, and Ohio.

9. My curriculum vitae is attached hereto as **Appendix A**. A list of all cases in which I have provided expert testimony in the last four years is attached hereto as **Appendix B**.

II. ALLEGATIONS AND ASSIGNMENT

10. I have been retained by Robbins, Russell, Englert, Orseck, Untereiner & Sauber LLP, counsel for Defendants Chain Bridge Bank, N.A. ("Chain Bridge" or "the Bank"), John J. Brough, and David M. Evinger (collectively, "Defendants"), in connection with the case captioned *Blue Flame Medical LLC v. Chain Bridge Bank, N.A., John J. Brough, and David M. Evinger,* No. 1:20-cv-00658 (E.D.V.A.).

11. Plaintiff Blue Flame Medical LLC ("Blue Flame Medical") brings claims related to a wire transfer of $456,888,600 originated on March 26, 2020 by the State of California (the "California Wire Transfer"), through its bank, JPMorgan Chase Bank, N.A. ("JPMorgan"), to Chain Bridge for the benefit of Blue Flame Medical.[1] The California Wire Transfer corresponded to the State of California's initial deposit on its purchase of 100 million N95 masks for

[1] Complaint, *Blue Flame Medical LLC v. Chain Bridge Bank, N.A., John J. Brough, and David M. Evinger*, Civil Action No. 20 Civ 658, (E.D.V.A. June 12, 2020) ("Complaint"), ¶¶ 1 - 3 and 61.

$609,161,000 (the "Blue Flame Transaction").[2] Chain Bridge personnel, aware that Blue Flame Medical had been formed only three days prior and had set up its account at Chain Bridge just the day before, communicated with officials from JPMorgan and the State of California about the wire transfer, and subsequently honored JPMorgan's request to return the wire transfer.[3]

12. Blue Flame Medical alleges that Chain Bridge's actions following its receipt of the California Wire Transfer resulted in substantial harm to Blue Flame Medical's business and the reputations of the company and its founders.[4] In particular, Blue Flame Medical alleges that Chain Bridge's communications with officials from the State of California amounted to defamation and tortious interference with Blue Flame Medical's contract and its future business with the State of California and other personal protective equipment ("PPE") purchasers.[5] In addition, Blue Flame Medical alleges that by honoring JPMorgan's request to return the wire transfer, Chain Bridge violated the FRB's Regulation J (which incorporates Article 4A of the Uniform Commercial Code ("U.C.C.")).[6]

13. Counsel for Chain Bridge asked me to apply my expertise in industry standards and practices relating to banking laws, regulations, and internal controls to the facts and circumstances at issue in this matter. Specifically, counsel asked me to assess, in light of federal banking laws and regulations and Chain Bridge's internal policies and procedures:

---

2 The initial deposit was approximately 75 percent of the total purchase price. Complaint, ¶¶ 25 and 61; Emails between John Thomas and Michael Wong, "Invoice," March 25, 2020, BFM000074110 - 111; Invoice from Blue Flame Medical LLC to Michael Wong, Contracts Administrator for the State of California - General Services Procurement Division, March 25, 2020, BFM000066431; Purchasing Authority Purchase Order from the State of California - General Services Procurement Division to Blue Flame Medical LLC, March 25, 2020, BFM000095501.

3 *See, e.g.*, *infra* Section IV.C and Section IV.D.

4 Complaint, ¶ 1.

5 Complaint, ¶¶ 2 - 3, 129, 138, and 168.

6 Complaint, ¶¶ 4, 87, 92 - 93, 96 - 97, and 109 - 112.

i. Whether the Blue Flame Transaction and California Wire Transfer exhibited characteristics of potentially suspicious and concerning activity under BSA/AML regulations and industry practices applying such regulations;

ii. Whether the actions taken by Chain Bridge personnel after opening Blue Flame Medical's account and receiving the California Wire Transfer were reasonable and consistent with industry standards and practices; and

iii. Whether Chain Bridge's planned use of an Insured Cash Sweep ("ICS") account or Certificate of Deposit Account Registry Service ("CDARS") account was consistent with industry practices for managing a large deposit into a customer's account.

14. All opinions expressed in this report are my own. I am not an attorney and offer no legal opinions. In preparing this report, I relied upon my education, experience, and knowledge of industry standards and practices concerning laws and regulations pertaining to account opening, funds transfer, transaction monitoring, and banks' other risk management requirements; documents produced in discovery and deposition testimony; and publicly available documents. A list of the materials that I considered in preparing my report is attached hereto as **Appendix C**.

15. Employees of Analysis Group, Inc., an economics, finance, and strategy consulting firm, working under my direction and supervision, assisted me with this assignment. I am being compensated at a rate of $850 per hour for my independent review and analysis provided in this case. This compensation is not contingent on the nature of my findings or the outcome of this litigation.

III. SUMMARY OF OPINIONS

16. Based on my analyses to date, as well as my education and experience, I conclude the following:

i. The Blue Flame Transaction and California Wire Transfer exhibited characteristics of potentially suspicious and concerning activity under BSA/AML regulations and industry practices applying such regulations, including Chain Bridge's own policies and procedures.

ii. The actions taken by Chain Bridge personnel after opening Blue Flame Medical's account and receiving the California Wire Transfer were reasonable and consistent with industry standards and practices. Specifically, the decisions by Chain Bridge personnel to communicate with the State of California to confirm information relating to the California Wire Transfer, to honor JPMorgan's request to return the California Wire Transfer, and to close the Blue Flame Medical-related accounts were reasonable and consistent with industry standards and practices.

iii. The initial steps that Chain Bridge took toward opening an ICS account and the Bank's consideration of a CDARS account are consistent with common industry practices. Midsize banks such as Chain Bridge frequently rely on ICS or CDARS accounts to maximize FDIC insurance when preparing to receive a large deposit into a customer's account.

17. My opinions, and the bases for my opinions, are presented in this report and the exhibit and appendices attached hereto. I hold all of my opinions as provided in this report to a reasonable degree of professional certainty. My work on this matter is ongoing, and I reserve the

right to supplement or amend my report should new information become available. I am prepared to testify at trial on the topics discussed in this report and to provide any additional relevant background. I also anticipate using certain demonstrative exhibits at trial to illustrate and support the concepts described in this report.

IV. BACKGROUND

A. Blue Flame Medical LLC

18. Blue Flame Medical was formed on March 23, 2020 by Michael Gula and John Thomas.[7] Mr. Gula is a co-founder of companies such as Mike Gula & Associates, a political fundraising and consulting firm; the Gula Graham Group, a political fundraising firm; and Prime Advocacy, a logistics firm for organizations seeking to schedule meetings on Capitol Hill and in state capitals.[8] Mr. Thomas is the founder and President of Thomas Partners Strategies, a political consulting and communications firm, and Thomas Partners Research, an opinion research firm, and is a television and radio personality.[9]

19. Blue Flame Medical advertised itself to be the largest global network of COVID-19 medical suppliers, with a focus in healthcare logistics and certified medical supplies.[10] The company advertised that it established a partnership with Great Health Companion Group to

---

7 State of Delaware Limited Liability Company Certificate of Formation for Blue Flame Medical LLC, March 23, 2020, CBB00002569 - 571; Complaint, ¶ 23; Blue Flame Medical Presentation, BFM000002416 - 430 at 418.

8 Complaint, ¶ 22; Blue Flame Medical Presentation, BFM000002416 - 430 at 419; Deposition of Michael Gula, January 12, 2021 ("Gula Deposition"), pp. 16:10 - 20:18; "About Us," Prime Advocacy, available at http://www.primeadvocacy.com/about-us, accessed February 3, 2021.

9 Complaint, ¶ 22; Blue Flame Medical Presentation, BFM000002416 - 430 at 420.

10 Blue Flame Medical Presentation, BFM000002416 - 430 at 417. *See also* Deposition of John Thomas, January 11, 2021 ("Thomas Deposition"), p. 282:12 - 15.

procure PPE.[11] Blue Flame Medical described Great Health Companion Group as a subsidiary of a majority owned and controlled Chinese State-Owned Enterprise ("SOE") that subcontracts with Chinese SOE PPE manufacturers.[12]

20. Blue Flame Medical is also affiliated with Blue Flame Strategies LLC ("Blue Flame Strategies"), a consulting entity formed on February 10, 2020 by Mr. Gula and Mr. Thomas, and Redline Strategies LLC ("Redline Strategies"), a consulting organization formed on March 16, 2020, also by Mr. Gula and Mr. Thomas.[13] Mr. Gula and Mr. Thomas testified that they formed Blue Flame Medical, a separate organization from these existing entities, in order to execute the Blue Flame Transaction.[14]

B. Chain Bridge Bank, N.A.

21. Chain Bridge is a nationally chartered, privately-held bank headquartered in McLean, Virginia that offers commercial and personal financial services.[15] Its primary deposit products are commercial and consumer checking accounts, and its primary lending products are consumer and commercial loans, including residential mortgages.[16]

---

11 Blue Flame Medical Presentation, BFM000002416 - 430 at 422 and 424.

12 Blue Flame Medical Presentation, BFM000002416 - 430 at 422.

13 State of Delaware Limited Liability Company Certificate of Formation for Blue Flame Strategies LLC, February 10, 2020, CBB00001198 - 199; Gula Deposition, p. 41:2 - 20; Thomas Deposition, pp. 56:9 - 57:14; State of Delaware Limited Liability Company Certificate of Formation for Redline Strategies LLC, March 16, 2020, CBB00001577 - 579.

14 Gula Deposition, p. 41:2 - 14; Thomas Deposition, pp. 56:9 - 57:14.

15 "Welcome Message from the Chairman," Chain Bridge Bank, N.A., available at https://www.chainbridgebank.com/connect-with-us/about-us/welcome-message-from-the-chairman, accessed February 3, 2021; "2019 Annual Report," Chain Bridge Bank, N.A., p. 7, available at https://www.chainbridgebank.com/assets/files/8TiiWnc7, accessed February 4, 2021.

16 "Welcome Message from the Chairman," Chain Bridge Bank, N.A., available at https://www.chainbridgebank.com/connect-with-us/about-us/welcome-message-from-the-chairman, accessed February 3, 2021; "2019 Annual Report," Chain Bridge Bank, N.A., p. 7, available at https://www.chainbridgebank.com/assets/files/8TiiWnc7, accessed February 4, 2021.

22. The Bank competes in a "niche market of specialized, large-scale commercial depositors."[17] Its commercial banking clients include advocacy and law firms, government contractors, certified public accountants, nonprofit organizations, political committees, property management firms, think tanks, and trade associations.[18] As of December 31, 2019, Chain Bridge's total assets amounted to $829.2 million and the Bank held deposits of $762.4 million.[19]

C. Opening of Blue Flame Medical's Account

23. Beginning on March 13, 2020, Mr. Gula emailed Chain Bridge personnel to open a checking account for Blue Flame Strategies.[20] On March 16 and March 17, Mr. Gula and Mr. Thomas completed and signed Blue Flame Strategies' account documents, including the Account Agreement, Unlawful Internet Gambling Notice & Certificate, Limited Liability Company Authorization Resolution, and Certification of Beneficial Owners of Legal Entities forms.[21]

24. On March 17, Mr. Gula emailed Maria Cole, Assistant Vice President and Commercial Relationship Manager at Chain Bridge, to open a checking account for Redline

[17] "2019 Annual Report," Chain Bridge Bank, N.A., p. iv, available at https://www.chainbridgebank.com/assets/files/8TiiWnc7, accessed February 4, 2021.

[18] "Commercial Banking," Chain Bridge Bank, N.A., available at https://www.chainbridgebank.com/commercial/commercial-banking, accessed February 3, 2021.

[19] "2019 Annual Report," Chain Bridge Bank, N.A., p. i, available at https://www.chainbridgebank.com/assets/files/8TiiWnc7, accessed February 4, 2021.

[20] Email from Michael Gula to Melissa Strano, cc'ing John Thomas, "Fwd: new business," March 13, 2020, CBB00001952; Email from Maria Cole to Michael Gula, cc'ing Mariano Castagnello, Mike Richardson, and Brad Ward, "Re: New Account," March 16, 2020, BFM000115483 - 487 at 483 - 484.

[21] Account Agreement between Chain Bridge Bank, N.A. and Blue Flame Strategies LLC, March 16, 2020, CBB00004391 - 392; Unlawful Internet Gambling Notice & Certificate for Blue Flame Strategies LLC, March 16, 2020, CBB00002617; Limited Liability Company Authorization Resolution between Chain Bridge Bank, N.A. and Blue Flame Strategies LLC, March 16, 2020, CBB00002618 - 621; Certification of Beneficial Owners of Legal Entities for Blue Flame Strategies LLC, March 17, 2020, CBB00002613 - 616.

Strategies, which he described to her as a "lobbying arm" at the "federal [and] state level."[22] Mr. Gula and Mr. Thomas completed and signed Redline Strategies' account documents the following day, including the Account Agreement, Certification of Beneficial Owners of Legal Entities, Unlawful Internet Gambling Notice & Certificate, and the Limited Liability Company Authorization Resolution forms.[23]

25. The following week, on the morning of March 25, Mr. Gula personally visited Chain Bridge's branch office, which was closed to customers due to COVID-19 quarantine procedures, to open an account for Blue Flame Medical.[24] Mr. Gula began the process of opening Blue Flame Medical's account with Mariano Castagnello, a Chain Bridge employee who was unfamiliar with Mr. Gula's other accounts.[25] Heather Schoeppe, Senior Vice President and Branch Manager at Chain Bridge, testified that neither she nor the Bank personnel who assisted Mr. Gula in opening Blue Flame Medical's account had assisted him with opening any of his existing accounts.[26] Ms. Schoeppe also testified that Mr. Gula normally worked with the Bank's

---

[22] Email from Michael Gula to Maria Cole, cc'ing John Thomas, "NEW business account needed," March 17, 2020, CBB00001574. Ms. Cole's title has been taken from her email signature. *See, e.g.*, Email from Maria Cole to Mike Richardson, cc'ing Heather Schoeppe and Wires, March 26, 2020, CBB00000686 - 695 at 689.

[23] Account Agreement between Chain Bridge Bank, N.A. and Redline Strategies LLC, March 18, 2020, CBB00004380 - 381; Certification of Beneficial Owners of Legal Entities for Redline Strategies LLC, March 18, 2020, CBB00002638 - 641; Unlawful Internet Gambling Notice & Certificate for Redline Strategies LLC, March 18, 2020, CBB00002637; Limited Liability Company Authorization Resolution between Chain Bridge Bank, N.A. and Redline Strategies LLC, March 18, 2020, CBB00002642 - 645.

[24] Deposition of David Evinger, January 29, 2021 ("Evinger Deposition"), pp. 129:19 - 130:12; Deposition of Heather Schoeppe, January 22, 2021 ("Schoeppe Deposition"), p. 46:1 - 21; Call between Heather Schoeppe and Mike Richardson, March 25, 2020, 9:23 a.m. ET, CBB00002792; Defendants' Responses to Plaintiff's First Set of Interrogatories, October 28, 2020, Response to Interrogatory No. 2, p. 3.

[25] Defendants' Responses to Plaintiff's First Set of Interrogatories, October 28, 2020, Response to Interrogatory No. 2, p. 3; Call between Mike Richardson, Heather Schoeppe and Mariano Castagnello, March 25, 2020, 10:13 a.m. ET, CBB00002783 ("I don't know why [Mr. Gula] came to the branch anyway, because he's been dealing with Maria [Cole] on other accounts").

[26] Schoeppe Deposition, pp. 17:21 - 18:4, 43:18 - 45:8.

"commercial deposit team, which is Mike Richardson and Maria Cole."[27] She noted that it was "strange" for Mr. Gula to open the account in person rather than work remotely with the commercial deposit team.[28]

26. During the account opening, Mr. Gula communicated to Mr. Castagnello that the expected monthly account activity would be as follows: five incoming foreign wires per month totaling $25 million, 25 incoming domestic wires per month totaling $75 million, and 50 outgoing domestic wires per month totaling $25 million.[29] Mr. Gula did not mention at that time that Blue Flame Medical expected a $450 million incoming wire into its account for that same day.[30]

27. Shortly before noon on March 25,[31] Mr. Castagnello forwarded to Ms. Cole a copy of the account documents that he had sent to Mr. Gula and Mr. Thomas via DocuSign for their signatures.[32] The Account Agreement, Certification of Beneficial Owners of Legal Entities, Limited Liability Company Authorization Resolution, and Unlawful Internet Gambling Notice & Certificate forms were completed and signed by Mr. Gula (but not Mr. Thomas) shortly after.[33] At

---

27 Schoeppe Deposition, pp. 44:11 - 44:16.

28 Schoeppe Deposition, pp. 43:3 - 43:10.

29 Email from Mariano Castagnello to Tsega Yohannes, "RE: Expected activity," March 27, 2020, CBB00001202 - 203.

30 Call between Heather Schoeppe and Michael Gula, March 25, 2020, 3:27 p.m. ET, CBB00002794; Call between Heather Schoeppe and Joanna Williamson, March 25, 2020, 4:25 p.m. ET, CBB00002797. *See also* Schoeppe Deposition, pp. 137:8 - 138:1 (identifying the call as the "first time" Ms. Schoeppe became aware of the amount of the wire).

31 For ease of reference, I have reported all time stamps contained in the documents cited in my report in Eastern Time.

32 Email from Mariano Castagnello to Maria Cole via DocuSign System, "Please DocuSign: Blue Flame Medical LLC," March 25, 2020, CBB00001518 - 519.

33 Account Agreement between Chain Bridge Bank, N.A. and Blue Flame Medical LLC, March 25, 2020, CBB00000555 - 556; Certification of Beneficial Owners of Legal Entities for Blue Flame Medical LLC, March 25, 2020, CBB00002546 - 549; Limited Liability Company Authorization Resolution between Chain Bridge Bank, N.A. and Blue Flame Medical LLC, March 25, 2020, CBB00002553 - 556; Unlawful Internet Gambling Notice & Certificate for Blue Flame Medical LLC, March 25, 2020, CBB00002557.

1:09 p.m., Mr. Gula emailed Mr. Castagnello Blue Flame Medical's articles of incorporation and EIN.[34]

D. The California Wire Transfer

1. The Blue Flame Transaction

28. On March 20, the week before Blue Flame Medical's account was opened, Mr. Thomas began his conversations with the State of California regarding the procurement and delivery of N95 masks.[35] On the evening of March 25, five days after discussions began and two days after Blue Flame Medical was formed, the State of California agreed to purchase 100 million N95 masks from Blue Flame Medical.[36]

29. The State of California agreed to pay $609,161,000, consisting of $476 million for the masks, $37,961,000 in sales tax, and $95,200,000 in shipping costs.[37] The State of California also agreed to a $456,888,600 initial deposit.[38] Blue Flame Medical prepared and sent an invoice

---

34 Email from Michael Gula to Mariano Castagnello, "Fwd: need BF Medical EIN/registration," March 25, 2020, CBB00002563 - 564; Notification of Employer Identification Number for Blue Flame Medical LLC, Internal Revenue Service, March 24, 2020, CBB00002565 - 567; State of Delaware Limited Liability Company Certificate of Formation for Blue Flame Medical LLC, March 23, 2020, CBB00002569 - 571.

35 Emails between John Thomas and Bill Simonson, March 20, 2020, "Re: FW: Email Connect - DGS and John Thomas," March 20, 2020, CBB00002221 - 289 at 230 - 234; Email from John Thomas to Bill Simonson, "Medical Supplies Listing," March 20, 2020, CBB00002221 - 289 at 236.

36 Emails between John Thomas and Michael Wong, "Invoice," March 25, 2020, BFM000074110 - 111; Invoice from Blue Flame Medical LLC to Michael Wong, Contracts Administrator for the State of California - General Services Procurement Division, March 25, 2020, BFM000066431.

37 Invoice from Blue Flame Medical LLC to Michael Wong, Contracts Administrator for the State of California - General Services Procurement Division to Blue Flame Medical LLC, March 25, 2020, BFM000066431.

38 Email from John Thomas to Michael Wong, "Re: Medical Supplies Sheet," March 24, 2020, CBB00002221 - 289 at 245 - 251; Purchasing Authority Purchase Order from the State of California - General Services Procurement Division to Blue Flame Medical LLC, March 25, 2020, BFM000095501.

for the State of California, and the State of California signed a purchase order the evening of March 25.[39]

2. Chain Bridge Personnel Learned of the California Wire Transfer and Discussed It Internally and with Blue Flame Medical

30. On March 25, at 3:27 p.m., Mr. Gula called Chain Bridge and spoke with Ms. Schoeppe.[40] Mr. Gula explained to her that "the state of California is sending an unbelievably large wire transfer in the amount of 450 million dollars" to Blue Flame Medical, and that Blue Flame Medical needs to be notified "the second it hits our account."[41] Immediately after the call, Ms. Schoeppe emailed Chain Bridge's Wires and Commercial Banking departments to inform them of the anticipated California Wire Transfer, explaining that Mr. Gula wished to be contacted "as soon as we receive the funds."[42]

31. Ms. Schoeppe called Mr. Gula at 4:16 p.m. to gather more information about the California Wire Transfer.[43] Minutes later, Ms. Schoeppe emailed John Brough, Chief Executive Officer at Chain Bridge, and Joanna Williamson, Chief Financial Officer at Chain Bridge, to

---

39 Emails between John Thomas and Michael Wong, "Invoice," March 25, 2020, BFM000074110 - 111; Invoice from Blue Flame Medical LLC to Michael Wong, Contracts Administrator for the State of California - General Services Procurement Division to Blue Flame Medical LLC, March 25, 2020, BFM000066431; Purchasing Authority Purchase Order from the State of California - General Services Procurement Division to Blue Flame Medical LLC, March 25, 2020, BFM000095501.

40 Call between Heather Schoeppe and Michael Gula, March 25, 2020, 3:27 p.m. ET, CBB00002794; Schoeppe Deposition, p. 18:5 - 8. For each of the calls that I cite to throughout the report, I rely on counsel's understanding of the list of participants and their full names, as well as the call's date and start time.

41 Call between Heather Schoeppe and Michael Gula, March 25, 2020, 3:27 p.m. ET, CBB00002794. *See also* Schoeppe Deposition, pp. 137:8 - 138:1 (identifying the call as the "first time" Ms. Schoeppe became aware of the amount of the wire).

42 Email from Heather Schoeppe to Wires, cc'ing Commercial Banking, "Blue Flame Medical incoming wire," March 25, 2020, CBB00000686 - 695 at 695.

43 Call between Heather Schoeppe and Michael Gula, March 25, 2020, 4:16 p.m. ET, CBB00002795.

inform them of the anticipated California Wire Transfer.[44] Ms. Schoeppe noted that Mr. Gula "said the money should be in today and will be spent out fairly rapidly as China produces the masks and [Blue Flame Medical] pay[s] them."[45]

32. Ms. Schoeppe then spoke with Ms. Williamson to provide additional detail on the California Wire Transfer.[46] She explained that Mr. Gula "showed up here this morning and was … panicked and … pushing us to open an account," and that Ms. Cole "didn't know either … about this 450 million to buy a hundred million masks … from China."[47] In response, Ms. Williamson stated, "we'll do whatever we need to do," and asked if it would be possible to place the funds in an ICS account.[48] An ICS account, or "Insured Cash Sweep" account, is frequently used by banks such as Chain Bridge. It would allow the Bank to distribute a portion of the California Wire Transfer among numerous other member financial institutions in the ICS Network in order to access FDIC insurance above the $250,000 per-account FDIC insurance limit for standard commercial bank accounts.[49] Ms. Schoeppe stated that she thought this would be possible, and offered to prepare the paperwork for the ICS account, which Ms. Williamson agreed to.[50]

---

44 Email from Heather Schoeppe to Mike Richardson, John Brough, and Joanna Williamson, "FW: Blue Flame Medical incoming wire 450 million," March 25, 2020, CBB00000686 - 695 at 693 - 694; Schoeppe Deposition, pp. 157:11 - 159:7; Deposition of John J. Brough, February 2, 2021 ("Brough Deposition"), p. 25:10 - 12, 29:10 - 12.

45 Email from Heather Schoeppe to Mike Richardson, John Brough, and Joanna Williamson, "FW: Blue Flame Medical incoming wire 450 million," March 25, 2020, CBB00000686 - 695 at 693 - 694.

46 Call between Heather Schoeppe and Joanna Williamson, March 25, 2020, 4:25 p.m. ET, CBB00002797.

47 Call between Heather Schoeppe and Joanna Williamson, March 25, 2020, 4:25 p.m. ET, CBB00002797.

48 Call between Heather Schoeppe and Joanna Williamson, March 25, 2020, 4:25 p.m. ET, CBB00002797.

49 *See* "IntraFi Network," ICS & CDARS, available at https://www.icsandcdars.com/about/intrafi-network-overview, accessed February 3, 2021; "How ICS and CDARS Work," ICS & CDARS, available at https://www.icsandcdars.com/how-it-works, accessed February 3, 2021. *See also* Section VIII.

50 Call between Heather Schoeppe and Joanna Williamson, March 25, 2020, 4:25 p.m. ET, CBB00002797.

33. At 4:32 p.m., Ms. Schoeppe was conferenced into a call with Mr. Brough and Mr. Evinger, President at Chain Bridge.[51] Ms. Schoeppe explained that Mr. Gula had "been calling all day," and was "just really anxious, dying to know when the money hits the account."[52] Mr. Brough subsequently stated that "if this is true, we can't hold that money on our balance sheet," and that Mr. Gula will "have to agree … to have it go into a CDARS account—or, to an ICS account."[53] A CDARS account, short for "Certificate of Deposit Account Registry Service," would similarly allow the Bank to hold a portion of the funds off-balance sheet in FDIC-insured accounts.[54] Mr. Evinger responded, "I guess we could ask [Blue Flame Medical] for any documentation regarding this transaction."[55] Mr. Evinger also stated that he would have the Bank's "[Bank Secrecy Act] team look at it too" and that he "[doesn't] like the smell of this."[56] Mr. Brough and Mr. Evinger agreed to call Mr. Gula.

34. A few minutes later, Mr. Brough and Mr. Evinger called Mr. Gula, who conferenced in his personal friend, Brent Case, to discuss the Blue Flame Transaction and California Wire Transfer.[57] According to Mr. Case's notes on the call, Mr. Gula conveyed that he

---

51 Call between John Brough, David Evinger, and Heather Schoeppe, March 25, 2020, 4:32 p.m. ET, CBB00002798; Schoeppe Deposition, pp. 166:17 - 167:8; Evinger Deposition, pp. 24:21 - 25:1.

52 Call between John Brough, David Evinger, and Heather Schoeppe, March 25, 2020, 4:32 p.m. ET, CBB00002798.

53 Call between John Brough, David Evinger, and Heather Schoeppe, March 25, 2020, 4:32 p.m. ET, CBB00002798.

54 Unlike an ICS account, which places funds into demand deposit or money market deposit accounts at other ICS Network member institutions, a CDARS account places funds into certificate of deposit accounts at other CDARS Network member institutions. *See* "IntraFi Network," ICS & CDARS, available at https://www.icsandcdars.com/about/intrafi-network-overview, accessed February 3, 2021; "How ICS and CDARS Work," ICS & CDARS, available at https://www.icsandcdars.com/how-it-works, accessed February 3, 2021. *See also* "IntraFi Network: Certificate of Deposit Account Registry Service, or CDARS," American Bankers Association, available at https://www.aba.com/member-tools/industry-solutions/endorsed-solutions/promontory-interfinancial-network-certificate-deposit-account-registry-service, accessed February 3, 2021.

55 Call between John Brough, David Evinger, and Heather Schoeppe, March 25, 2020, 4:32 p.m. ET, CBB00002798.

56 Call between John Brough, David Evinger, and Heather Schoeppe, March 25, 2020, 4:32 p.m. ET, CBB00002798.

57 Defendants' Responses to Plaintiff's First Set of Interrogatories, October 28, 2020, Responses to Interrogatory No. 2, p. 2; Gula Deposition, p. 159:1 - 8; Evinger Deposition, p. 189:3 - 15.

understood it was hard for the Bank to believe that he could transition from a business with annual deposits in hundreds of thousands of dollars to one with transactions in hundreds of millions.[58] Mr. Case recalled that Mr. Brough and Mr. Evinger proposed the use of an ICS account so that the proceeds "would be covered by FDIC insurance," and informed Mr. Gula that "further documentation about [Blue Flame Medical] would be useful."[59] Mr. Evinger also testified that he and Mr. Brough specifically requested "copies of [the] contracts" with the State of California and with Mr. Gula's manufacturer.[60]

35. Following the call, Mr. Evinger emailed Mr. Gula, stating, "[w]e look forward to receiving your information related to these contracts."[61] Mr. Gula responded to Mr. Brough, asking if the Bank could "check on [their] end about the wire. [M]y partner was with the [California procurement] officer when [the officer] hit send," indicating that he expected that the Bank may have already received the wire transfer.[62]

36. Later that evening, Mr. Brough asked Mr. Gula via email if he "sen[t] any money to China or others as a 'fee' for these transactions," to which Mr. Gula responded, "no, we have not sent the money to [C]hina but when we do this is where we are sending it," attaching wire instructions for a beneficiary named Wingar Industrial Inc, with a header listing Great Health

---

58 Email from Michael Gula to Brielle Appelbaum, "Fwd: My memory of the call with Chain Bridge Bank," May 9, 2020, BFM000137279 - 280 at 279.

59 Email from Michael Gula to Brielle Appelbaum, "Fwd: My memory of the call with Chain Bridge Bank," May 9, 2020, BFM000137279 - 280 at 280. *See also* Evinger Deposition, p. 194:6 - 12; Brough Deposition p. 355:3 - 17.

60 Evinger Deposition, p. 202:11 - 13. *See also* Brough Deposition, pp. 142:10 - 18, 143:3 - 9. *See also* Brough Typed Notes, CBB00004463 - 467 at 464 ("David asked [Mr. Gula] for a copy of any contracts he had in place with purchasers or sellers").

61 Email from David Evinger to Michael Gula, cc'ing John Brough, "Contact Info," March 25, 2020, BFM000013445 - 447 at 446.

62 Email from Michael Gula to David Evinger, cc'ing John Brough, "RE: Contact Info," March 25, 2020, BFM000013445 - 447 at 446.

Companion Group.[63] Upon an Internet search for Wingar Industrial Inc., Mr. Evinger discovered that the company was a cutlery and flatware retailer.[64]

37. Shortly thereafter, Mr. Gula also sent Mr. Evinger and Mr. Brough a screenshot of an email sent by "Wong, Michael@DGS" to Mr. Thomas, which stated that the "[California] State Controllers [sic] Office will be paying you via wire transfer first thing in the morning."[65] In his deposition, Mr. Evinger noted that he did not "consider this to be what [Chain Bridge] requested" and that it "wouldn't suffice" as documentation for the transaction. Mr. Evinger also explained that the requested contracts were "an important part of [Chain Bridge's] due diligence," and the screenshot "isn't a contract" or an "official form."[66]

38. Around the same time, Ms. Schoeppe emailed Mike Richardson, Senior Vice President and Commercial Banking Manager at Chain Bridge, explaining that Mr. Brough and Mr. Evinger "are very skeptical about this ... [t]hey just think it seems very strange a company established 2 days ago would get awarded this huge contract from California."[67] In the same exchange, Ms. Schoeppe noted that Mr. Brough and Mr. Evinger discussed setting up an ICS

---

63 Emails between John Brough, David Evinger, and Michael Gula, "RE: Contact Info," March 25, 2020, BFM000013445 - 447 at 445; Wiring Instructions from Great Health Companion Group Ltd. Co. for Beneficiary Wingar Industrial Inc., BFM000013448.

64 Brough Deposition, pp. 159:18 - 160:2, 161:11 - 14. *See also* "Welcome," Wingar Industrial Inc., available at https://wingar.com/, accessed February 10, 2021.

65 Email from Michael Gula to David Evinger and John Brough, "Screenshot 2020-03-25 at 6.26.08 PM," March 25, 2020, CBB00002699. Screenshot sent by Michael Gula to David Evinger and John Brough, March 25, 2020, CBB00002700.

66 Evinger Deposition, pp. 222:8 - 223:8.

67 Email from Heather Schoeppe to Mike Richardson, "RE: Blue Flame Medical incoming wire 450 million," March 25, 2020, CBB00000686 - 695 at 692. *See also* Schoeppe Deposition, pp. 194:19 - 195:10.

account.[68] Mr. Richardson subsequently corresponded with Ms. Cole through the next morning to set up the ICS account.[69]

3. Chain Bridge Received the California Wire Transfer and Communicated with JPMorgan and the State of California

39. On March 26, at 8:40 a.m., Mr. Gula sent Mr. Evinger an email with a link to Blue Flame Medical's website.[70] Mr. Evinger testified that this still did not satisfy his request for Mr. Gula to provide the underlying documentation on the Blue Flame Transaction as part of the Bank's due diligence.[71]

40. Later that morning, Mr. Thomas called Ms. Cole multiple times to inquire whether the California Wire Transfer had "already hit their account."[72] At 11:02 a.m., Mr. Thomas called Ms. Cole and asked for a Chain Bridge employee to stay on the line until the wire transfer came through.[73] He explained that he was "just dying to know when the wire lands in our account" and "confidentially" disclosed that Blue Flame Medical planned to move "several billion dollars" through the account over the next few weeks.[74] He called again at 11:51 a.m. and 11:59 a.m. to inquire about the wire transfer, explaining that he was a "ball of nerves."[75]

---

68 Email from Heather Schoeppe to Mike Richardson, "RE: Blue Flame Medical incoming wire 450 million," March 25, 2020, CBB00000686 - 695 at 692.

69 Emails between Mike Richardson and Maria Cole, cc'ing Heather Schoeppe, "RE: Blue Flame Medical incoming wire 450 million," March 25 - 26, 2020, CBB00000686 - 695 at 689 - 691.

70 Email from Michael Gula to David Evinger. "Blue Flame Medical | Fighting Coronavirus," March 26, 2020, CBB00002686.

71 Evinger Deposition, p. 228:17 - 19 ("My discussion with [Mr. Gula] was about --about the contracts themselves, not about his website").

72 Emails between Mike Richardson and Maria Cole, cc'ing Heather Schoeppe, "Re: Blue Flame Medical incoming wire 450 million," March 25 - 26, 2020, CBB00000686 - 695 at 689.

73 Call between Maria Cole and John Thomas, March 26, 2020, 11:02 a.m. ET, CBB00002786.

74 Call between Maria Cole and John Thomas, March 26, 2020, 11:02 a.m. ET, CBB00002786.

75 Call between Maria Cole and John Thomas, March 26, 2020, 11:51 a.m. ET, CBB00002787; Call between Maria Cole and John Thomas, March 26, 2020, 11:59 a.m. ET, CBB00002788.

41. At 11:55 a.m., Chain Bridge received a Fedwire Funds Processor Message detailing that the California Wire Transfer had been received.[76] Four minutes later, Mr. Gula received an automated email from Chain Bridge's Wire Department detailing the incoming wire transfer.[77]

42. Within 12 minutes of the wire transfer's receipt, Mr. Evinger emailed Chain Bridge personnel to "[p]lace HOLD on funds," and a few minutes after, Mr. Brough stated, "[d]o not contact the client about this wire."[78] Ms. Schoeppe responded, stating that Mr. Gula "is calling us so much" and "is extremely aggressive and will not hang up."[79]

43. Around the same time, at 12:14 p.m., Mr. Thomas and Ethan Bearman, Blue Flame Medical's counsel—who was not a signer on Blue Flame Medical's account—emailed Ms. Cole to initiate the paperwork for an outbound wire transfer of $22.68 million to Suuchi Inc., stating that the outgoing wire transfer needed to get "out the door asap."[80] Ms. Cole forwarded the email to Mr. Brough, Mr. Evinger, and Mr. Richardson, stating, "[l]ooking forward to your instructions.

---

76 Fedwire Funds Processor Message, March 26, 2020 at 11:55 a.m., CBB00002779. Blue Flame Medical and the State of California originally intended for the California Wire Transfer to occur the same evening, but they missed the cut off time. As a result, the State of California agreed to send the California Wire Transfer the following morning. *See* Email from Allan Watson to Jim Spano et al., "email chain restored w/all who need to know…..," March 25, 2020, CBB00002124 - 125 at 125; Emails between Michael Gula and Maria Cole, "wire," March 25, 2020, CBB00001433 - 436 at 433 - 434; Emails between Michael Gula and David Evinger, cc'ing John Brough, "Contact Info," March 25, 2020, BFM000013445 - 447 at 446.

77 Email from Chain Bridge Bank N.A., Wire Department to Michael Gula, "Incoming Wire Confirmation," March 26, 2020, CBB00001938.

78 Email from David Evinger to Jennifer Lincoln, John Brough, and Farrukh Memon, cc'ing Wires, "RE: Incoming Large Wire," March 26, 2020, CBB00000728 - 729 at 728; Email from John Brough to Jennifer Lincoln, David Evinger, Joanna Williamson, Farrukh Memon, Heather Schoeppe, and Mike Richardson, cc'ing Wires, "RE: Incoming Large Wire," March 26, 2020, CBB00000741 - 743 at 742.

79 Email from Heather Schoeppe to Thais Ribeiro, John Brough, David Evinger, and Mike Richardson, cc'ing Wires, "RE: Incoming Large Wire," March 26, 2020, CBB00000741 - 743 at 741; Email from Heather Schoeppe to John Brough, Jennifer Lincoln, David Evinger, Joanna Williamson, Farrukh Memon, and Mike Richardson, cc'ing Wires, "RE: Incoming Large Wire," March 26, 2020, CBB00000741 - 743 at 741 - 742. *See also* Schoeppe Deposition, pp. 106:21 - 107:14 and 248:17 - 249:9.

80 Email from John Thomas to Ethan Bearman, cc'ing Maria Cole and Michael Gula, "Re: Blue Flame Medical LLC-Wire Transfer," March 26, 2020, CBB00000655 - 657 at 656; Account Agreement between Chain Bridge Bank, N.A. and Blue Flame Medical LLC, March 25, 2020, CBB00000555 - 556.

Until then I won't reply or answer their calls."[81] Mr. Gula continued to call "non-stop" through the afternoon.[82]

44. At 12:31 p.m., Tim Coffey, Vice President in the Payments Control Department at JPMorgan, called Chain Bridge and reached Mr. Castagnello.[83] According to Mr. Coffey, the intent of the call was to get Chain Bridge to place the funds on hold.[84] Mr. Coffey requested to speak with individuals in Chain Bridge's fraud or wire transfer departments because JPMorgan had "concerns of fraud" regarding the California Wire Transfer.[85] Mr. Coffey was subsequently transferred to Mr. Evinger.[86] Mr. Coffey reported to Mr. Evinger that JPMorgan had suspicions regarding the California Wire Transfer and wanted Chain Bridge hold the funds, to which Mr. Evinger responded that Chain Bridge had similar concerns and had already placed the funds on hold.[87]

45. At 12:44 p.m., Rakesh Korpal, Executive Director, Wholesale Payments Operations, Corporate and Investment Bank at JPMorgan, called Mr. Brough and Mr. Evinger to notify them that the California Wire Transfer had been flagged by JPMorgan's Global Securities Investigation Team.[88] He reported that the Global Securities Investigations Team "is coming back

---

81 Email from Maria Cole to John Brough, David Evinger, and Mike Richardson, "FW: Blue Flame Medical LLC - Wire Transfer," March 26, 2020, CBB00000655 - 657 at 655 - 656.

82 Email from Heather Schoeppe to Maria Cole, John Brough, David Evinger, and Mike Richardson, "RE: Blue Flame Medical LLC- Wire Transfer," March 26, 2020, CBB00000655 - 657 at 655.

83 Call between Mariano Castagnello and Tim Coffey, March 26, 2020, 12:31 p.m. ET, CBB00002784; Deposition of Timothy Coffey (Rough), February 11, 2021 ("Coffey Deposition"), p. 15:7 - 12.

84 Coffey Deposition, p. 65:10 - 16.

85 Call between Mariano Castagnello and Tim Coffey, March 26, 2020, 12:31 p.m. ET, CBB00002784. *See also* Coffey Deposition, pp. 82:6 - 83:22; Deposition of Rakesh Korpal, a 30(b)(6) Witness, February 9, 2021 ("Korpal Deposition"), p. 222:17 - 22.

86 Coffey Deposition, p. 64:2 - 7.

87 Coffey Deposition, pp. 64:13 - 66:4.

88 Call between David Evinger, John Brough and Rakesh Korpal, March 26, 2020, 12:44 p.m. ET, CBB00002541 - 542 at 541. Mr. Korpal's title has been taken from his email signature. *See, e.g.*, Email from Rakesh Korpal to

to [him] and saying that this does not look right," and that research on the transaction was "all leading to not-good places."[89]

46. While Mr. Brough and Mr. Evinger were on the phone with Mr. Korpal, Fee Chang from the California Department of General Services left Mr. Evinger a voicemail, confirming the transferred sum and stating that she could "confirm that this is a … legitimate … transfer."[90] Mr. Brough and Mr. Evinger promptly returned Ms. Chang's call. During that call, Mr. Evinger requested "documentation to support [the California Wire Transfer]," and Ms. Chang offered to put Chain Bridge in touch with Natalie Gonzales at the California State Treasurer's Office, whom Chang described as "the one … in charge of the transfers."[91]

47. At around 1:19 p.m., Mr. Evinger and Mr. Brough spoke with Mark Hariri and Natalie Gonzales from the California State Treasurer's Office.[92] Mr. Evinger testified that the call was "to confirm that the wire was … properly authorized … that the funds were intended to go to Blue Flame Medical, and [that the State of California] knew … about the overall transaction"[93] According to Mr. Brough and Mr. Evinger, Mr. Hariri and Ms. Gonzales sounded "surprised" to learn that Blue Flame Medical was a newly-formed entity with an account that had been opened

---

Jenifer Robinson, Timothy Coffey, Akhil Kedia, and Nikki Ticzon, "FW:," March 27, 2020, JPMC-00000239 - 240 at 239. *See also* Korpal Deposition, pp. 30:20 - 31:1.

89 Call between David Evinger, John Brough and Rakesh Korpal, March 26, 2020, 12:44 p.m. ET, CBB00002541 - 542 at 541.

90 Voicemail from Fee Chang to David Evinger, March 26, 2020, 12:52 p.m. ET, CBB00000707.

91 Call between David Evinger, John Brough, and Fee Chang, March 26, 2020, 12:55 p.m. ET, CBB00002543.

92 Deposition of Natalie Gonzales, January 28, 2021 ("Gonzales Deposition"), pp. 48:22 - 49:20; Evinger Deposition, pp. 249:22 - 250:7; Brough Deposition, pp. 278:18 - 279:7; Defendants' Responses to Plaintiff's First Set of Interrogatories, October 28, 2020, Response to Interrogatory No. 2, p. 4. Ms. Gonzales recalls speaking only with Mr. Evinger, but Mr. Evinger and Mr. Brough each recall that both of them were on the call.

93 Evinger Deposition, pp. 250:20 - 251:2.

the previous day by political operatives.[94] Ms. Gonzales testified that she and Mr. Hariri asked if the wire had been credited to Blue Flame Medical's account and requested that Mr. Evinger hold the funds until the California State Treasurer's Office could obtain additional information and relay it to the California Department of General Services.[95]

48. At 1:35 p.m., Mr. Korpal called Mr. Brough and Mr. Evinger and informed them that California officials were still "a bit unsure" about the California Wire Transaction.[96] Mr. Evinger asked JPMorgan about the possibility of a recall.[97] Mr. Korpal said that he "can issue a recall," but that he was "comfortable that you're holding the money right now."[98] He asked Chain Bridge to "give [him] a few more minutes."[99] Minutes later, Mr. Coffey called Mr. Brough and Mr. Evinger, stating that JPMorgan had "enough concerns that we feel we need to claw those funds back."[100] Mr. Coffey asked, "[d]o you need a recall message from us, or what are you looking for from us?"[101] Mr. Evinger requested "official communication from [JPMorgan] to [Chain Bridge] to recall the funds," and Mr. Coffey confirmed that a communication over the Fedline platform would be sent "in the next couple of minutes."[102]

94 Evinger Deposition, p. 282:10 - 14; Brough Deposition, pp. 283:9 - 284:21.

95 Gonzales Deposition, pp. 50:7 - 15, 52:8 - 19.

96 Call between David Evinger, John Brough and Rakesh Korpal, March 26, 2020, 1:35 p.m. ET, CBB00002544; Brough Deposition, p. 258:8 - 10.

97 Call between David Evinger, John Brough and Rakesh Korpal, March 26, 2020, 1:35 p.m. ET, CBB00002544.

98 Call between David Evinger, John Brough and Rakesh Korpal, March 26, 2020, 1:35 p.m. ET, CBB00002544.

99 Call between David Evinger, John Brough and Rakesh Korpal, March 26, 2020, 1:35 p.m. ET, CBB00002544.

100 Call between David Evinger, John Brough and Tim Coffey, March 26, 2020, 1:37 p.m. ET, CBB00002545.

101 Call between David Evinger, John Brough and Tim Coffey, March 26, 2020, 1:37 p.m. ET, CBB00002545.

102 Call between David Evinger, John Brough and Tim Coffey, March 26, 2020, 1:37 p.m. ET, CBB00002545.

4. Chain Bridge Honored JPMorgan's Request to Return the California Wire Transfer and Closed the Blue Flame Medical Account

49. At 2:05 p.m., JPMorgan sent Chain Bridge a Fedwire Funds Processor message requesting the return of the California Wire Transfer.[103] Claudia Mojica, an Operations Technician at Chain Bridge, informed Mr. Brough, Mr. Evinger, and Thais Ribeiro, Vice President and Director of Operations, of the message at 2:13 p.m., and Mr. Brough directed Ms. Mojica to return the wire at 2:26 p.m.[104] Mr. Brough subsequently instructed Ms. Schoeppe to "close the BlueFlame [sic] accounts."[105] Ms. Schoeppe closed the Blue Flame Strategies and Redline Strategies accounts, and stated that she would "close Blue Flame Medical once the wire is returned."[106]

50. At the same time, Mr. Brough and Mr. Evinger communicated with Mr. Gula regarding the California Wire Transfer. Mr. Brough responded to Mr. Gula's prior emails, stating, "[w]e received official notice from the sending bank to return the wire. Please resolve directly with the state of California."[107] Around 2:30 p.m., Mr. Brough and Mr. Evinger met with Mr. Gula outside Chain Bridge and discussed the California Wire Transfer, JPMorgan's cancellation of it, and the closing of Blue Flame Medical's account.[108] In his deposition, Mr. Brough testified that

---

[103] Fedwire Funds Processor Message, March 26, 2020 at 2:05 p.m., CBB00002780.

[104] Email from Claudia Mojica to John Brough, David Evinger and Thais Ribeiro, "Message from JPMorgan Chase - Large Incoming Wire," March 26, 2020, CBB00000613 - 615 at 614 - 615.

[105] Email from John Brough to Heather Schoeppe, Maria Cole, Mike Richardson, Mariano Castagnello and Angeli Nanali, cc'ing David Evinger, Thais Ribeiro, Joanna Williamson, and Betsy Sharon, "Please close BlueFlame Accounts," March 26, 2020, CBB00002508 - 512 at 511.

[106] Email from Heather Schoeppe to John Brough, Maria Cole, Mike Richardson, Mariano Castagnello and Angeli Nanali, cc'ing David Evinger, Thais Ribeiro, Joanna Williamson, and Betsy Sharon, "RE: Please close BlueFlame Accounts," March 26, 2020, CBB00002508 - 512 at 509 - 511.

[107] Email from John Brough to Michael Gula and David Evinger, "RE: Contact Info," March 26, 2020, BFM000074101 - 106 at 101 - 102.

[108] Defendants' Responses to Plaintiff's First Set of Interrogatories, October 28, 2020, Response to Interrogatory No. 2, p. 5. Mr. Brough and Mr. Evinger met with Mr. Gula in person because he had emailed Mr. Evinger approximately 15 minutes prior, notifying him that he was coming to the Bank. *See* Email from Michael Gula to David Evinger, "Coming in. Are you there?," March 26, 2020, CBB00000639.

Mr. Gula did not object to the cancellation.[109] Within an hour of that meeting, at 3:21 p.m., Chain Bridge honored JPMorgan's cancellation request by returning the California Wire Transfer.[110]

V. CHAIN BRIDGE BANK IS SUBJECT TO FEDERAL BANKING LAWS AND REGULATIONS AND INTERNAL POLICIES AND PROCEDURES THAT GOVERN ITS WIRE TRANSFER ACTIVITIES

51. In the remainder of this report, I assess the actions taken by Chain Bridge personnel after opening Blue Flame Medical's checking account and receiving the California Wire Transfer within the context of industry standards and practices and the regulatory context at the time. In conducting this assessment, I consider the applicable laws and regulations as well as Chain Bridge's internal policies and procedures.

52. Chain Bridge provides its customers with the ability to transfer funds to, and receive funds from, other domestic and international financial institutions by wire.[111] In practice, banks that engage in such activities are subject to federal and state laws and regulations governing wire transfers, including the requirements of BSA/AML regulations, the USA PATRIOT Act, Regulation J and all other requirements by the FRB applicable to wire transfers sent through its Fedwire system, and any internal policies and procedures that banks develop to comply with these laws and regulations.[112]

---

109 Brough Deposition, p. 328:1 - 16.

110 Fedwire Funds Processor Message, March 26, 2020 at 3:21 p.m., CBB00002781.

111 *See, e.g.*, Wire Transfer Policy, Chain Bridge Bank, N.A., January 2020, CBB00004294 - 301 at 295.

112 *See, e.g.*, Wire Transfer Policy, Chain Bridge Bank, N.A., January 2020, CBB00004294 - 301 at 295; Bank Secrecy Act, Anti Money Laundering Control, and Office of Foreign Assets Control Policy, Chain Bridge Bank, N.A., March 2020, CBB00004235 - 273 at 236.

A. Federal Regulators Develop and Enforce a Series of Laws and Regulations to Ensure the Safety and Soundness of the Banking System

53. The primary objective of federal regulators and related entities such as the OCC, FRB, FDIC, and FinCEN is safety and soundness in the banking system; that is, to ensure that banks are able to contain risks and prevent the occurrence of illicit activities (e.g., fraud or money laundering).[113] Federal regulators achieve this objective through an interlocking set of laws and regulations pertaining to fraud prevention and regulatory and legal compliance, and through prudential supervision of banks' risk management procedures and internal controls.[114] In turn, banks develop policies, procedures, and other internal controls to ensure that they comply with all laws and regulations.[115] The federal laws and regulations governing wire transfers include BSA/AML regulations, the USA PATRIOT Act, and the FRB's Regulation J, each of which I describe below.

1. BSA/AML Regulations

54. The Currency and Foreign Transactions Reporting Act of 1970 (commonly known as the Bank Secrecy Act, or BSA) requires U.S. financial institutions to assist U.S. government

---

113 *See, e.g.*, "Safety and Soundness," Federal Reserve Bank of St. Louis, available at https://www.stlouisfed.org/in-plain-english/safety-and-soundness, accessed February 5, 2021; "Examinations Overview," Office of the Comptroller of the Currency, available at https://www.occ.treas.gov/topics/supervision-and-examination/examinations/examinations-overview/index-examinations-overview.html, accessed February 5, 2021; "Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision," Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, July 22, 2019, available at https://www.fincen.gov/sites/default/files/2019-07/Joint%20Statement%20on%20Risk-Focused%20Bank%20Secrecy%20Act-Anti-Money%20Laundering%20Supervision%20FINAL1.pdf, accessed February 9, 2021.

114 *See, e.g.*, "Safety and Soundness," Federal Reserve Bank of St. Louis, available at https://www.stlouisfed.org/in-plain-english/safety-and-soundness, accessed February 5, 2021; "Examinations Overview," Office of the Comptroller of the Currency, available at https://www.occ.treas.gov/topics/supervision-and-examination/examinations/examinations-overview/index-examinations-overview.html, accessed February 5, 2021.

115 *See, e.g.*, Wire Transfer Policy, Chain Bridge Bank, N.A., January 2020, CBB00004294 - 301 at 295; Bank Secrecy Act, Anti Money Laundering Control, and Office of Foreign Assets Control Policy, Chain Bridge Bank, N.A., March 2020, CBB00004235 - 273 at 236.

agencies in detecting and preventing potentially fraudulent transactions and other account activity that may indicate illicit activities.[116] The BSA may also be referred to as an anti-money laundering law (AML), or jointly as BSA/AML.[117]

55. Financial institutions subject to BSA/AML regulations look to the Federal Financial Institutions Examination Counsel's ("FFIEC's") BSA/AML Manual for guidance.[118] The BSA/AML Manual outlines a list of "potentially suspicious activities" that banks and examiners rely on to identify transactions that would raise reasonable suspicion as part of banks' transaction monitoring procedures.[119] The existence of one of these activities is not by itself proof

[116] *See, e.g.*, "FinCEN's Mandate from Congress," Financial Crimes Enforcement Network, available at https://www.fincen.gov/resources/statutes-regulations/fincens-mandate-congress, accessed February 5, 2021.

[117] "FinCEN's Mandate from Congress," Financial Crimes Enforcement Network, available at https://www.fincen.gov/resources/statutes-regulations/fincens-mandate-congress, accessed February 5, 2021.

[118] The FFIEC's BSA/AML Manual was released in 2005, and has been revised in 2006, 2007, 2010, 2014, and, most recently, in April 2020. I rely on the FFIEC's BSA/AML Manual as of 2014, which was in place as of the California Wire Transfer. *See* Bank Secrecy Act/Anti-Money Laundering Examination Manual ("BSA/AML Manual"), Federal Financial Institutions Examination Council, 2014, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021; "For Immediate Release," Federal Financial Institutions Examination Council, June 30, 2005, available at https://www.ffiec.gov/press/pr063005.htm, accessed February 11, 2021; "Agencies Release Revised Bank Secrecy Act/Anti-Money Laundering Examination Manual," Federal Financial Institutions Examination Council, July 28, 2006, available at https://www.ffiec.gov/press/pr072806.htm, accessed February 11, 2021; "Agencies Release Revised Bank Secrecy Act/Anti-Money Laundering Examination Manual," Federal Financial Institutions Examination Council, August 24, 2007, available at https://www.ffiec.gov/press/pr082407.htm, accessed February 11, 2021; "Agencies Release Revised Bank Secrecy Act/Anti-Money Laundering Examination Manual," Federal Financial Institutions Examination Council, April 29, 2010, available at https://www.ffiec.gov/press/pr042910.htm, accessed February 11, 2021; "Financial Regulators Release 2014 Bank Secrecy Act/Anti-Money Laundering Examination Manual," Federal Financial Institutions Examination Council, December 2, 2014, available at https://www.ffiec.gov/press/pr120214.htm, accessed February 11, 2021; "April 2020 Updates to the Bank Secrecy Act/Anti-Money Laundering Examination Manual," Board of Governors of the Federal Reserve System, Federal Deposit Insurance Company, National Credit Union Association, Office of the Comptroller of the Currency, State Liaison Committee, April 15, 2020, available at https://www.ffiec.gov/press/PDF/Interagency%20Statement.pdf, accessed February 11, 2021.

[119] "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

of illicit conduct, but is understood as warranting additional scrutiny when encountered.[120] Under the BSA/AML Manual, such additional scrutiny "should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose."[121] Examples of these potentially suspicious activities include, but are not limited to:[122]

i. "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;"

ii. "The customer's background differs from that which would be expected on the basis of his or her business activities;"

iii. "Funds transfer activity is unexplained, repetitive, or shows unusual patterns;"

iv. "Payments or receipts with no apparent links to legitimate contracts, goods, or services are received;"

v. The customer is "conducting business in higher-risk jurisdictions;"

---

120 "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. F-1, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

121 "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. F-1, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

122 "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, pp. F-1, F-2, F-3, F-5, and F-8, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

vi. The "[c]ustomer has established multiple accounts in various corporate or individual names that lack sufficient business purpose for the account complexities or appear to be an effort to hide the beneficial ownership from the bank;" and

vii. The "[c]ustomer makes high-value transactions not commensurate with the customer's known incomes."

56. Banks also heed FinCEN advisories that "contain[] examples of 'red flags' to inform and assist banks" in identifying potentially suspicious activities.[123] For example, FinCEN has issued guidance for adhering to BSA/AML regulations by requiring "financial institutions to establish and maintain written policies and procedures that are reasonably designed to…conduct ongoing monitoring to identify and report suspicious transactions."[124] Such guidance aligns with the BSA/AML Manual's requirement that banks' policies and procedures "[p]rovide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity."[125]

57. In my experience, banks that facilitate large transactions must be mindful of safety-and-soundness concerns about potentially suspicious activity that are set out in the BSA/AML regulations in order to avoid civil and criminal liability for facilitating illicit transactions.[126] Banks that monitor their customers' accounts for such activity would not complete transactions after

[123] "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. F-1, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

[124] "FinCEN Reminds Financial Institutions that the CDD Rules Becomes Effective Today," Financial Crimes Enforcement Network, May 11, 2018, available at https://www.fincen.gov/news/news-releases/fincen-reminds-financial-institutions-cdd-rule-becomes-effective-today, accessed February 9, 2021.

[125] "BSA/AML Compliance Program — Overview," BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, pp. 29 - 30, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

[126] *See also* "Background," BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. 3, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

having recognized the characteristics of potentially suspicious activity and before resolving such concerns to their satisfaction. Banks that allow transactions to proceed without resolving concerns about potentially suspicious activity have been the target of regulatory investigations, some of which have resulted in criminal prosecutions, deferred prosecution agreements, significant fines, and other sanctions.[127]

2. The USA PATRIOT Act

58. Several AML laws have been enacted and amended to strengthen the BSA, most significantly the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "USA PATRIOT Act").[128] The USA PATRIOT Act requires regulatory agencies to enact regulations further delineating the requirement for financial institutions to cooperate with other financial institutions, regulatory authorities, and law enforcement authorities to report potentially suspicious transactions and deter illicit activities.[129]

59. For example, banks adhere to (among other provisions) Section 314 of the USA PATRIOT Act, which details financial institutions' cooperative efforts to share information

---

[127] *See, e.g.*, "FinCEN Announces $390,000,000 Enforcement Action Against Capital One, National Association for Violations of the Bank Secrecy Act," Financial Crimes Enforcement Network, January 15, 2021, available at https://www.fincen.gov/news/news-releases/fincen-announces-390000000-enforcement-action-against-capital-one-national, accessed February 5, 2021; Order to Pay, In the Matter of Apple Bank for Savings, Case No. FDIC-19-0201k, December 21, 2020, available at https://orders.fdic.gov/sfc/servlet.shepherd/document/download/069t000000IEJH6AAP?operationContext=S1, accessed February 5, 2021; "FinCEN Assesses $14.5 Million Penalty against UBS Financial Services for Anti-Money Laundering Failures," Financial Crimes Enforcement Network, December 17, 2018, available at https://www.fincen.gov/news/news-releases/fincen-assesses-145-million-penalty-against-ubs-financial-services-anti-money, accessed February 5, 2021; "OCC Assesses $50 Million Civil Money Penalty and Terminates Consent Order Against Rabobank, N.A.," Office of the Comptroller of the Currency, February 7, 2018, available at https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-15.html, accessed February 5, 2021; "Rabobank NA Pleads Guilty, Agrees to Pay Over $360 Million," United States Department of Justice, February 7, 2018, available at https://www.justice.gov/opa/pr/rabobank-na-pleads-guilty-agrees-pay-over-360-million, accessed February 10, 2021.

[128] Public Law 107-56, 115 Stat. 272 (Oct. 26, 2001) ("USA PATRIOT Act").

[129] USA PATRIOT Act, §§ 312, 314, and 326.

regarding potentially suspicious activities.[130] Section 314(a) allows for "regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected based on credible evidence of engaging in" potentially suspicious activities, while Section 314(b) allows for this information sharing between two or more financial institutions.[131]

60. In my experience, banks apply the USA PATRIOT Act's provisions regarding potentially suspicious activities and transactions consistent with the analogous requirements of other BSA/AML regulations. As with other BSA/AML regulations, banks do not complete or otherwise facilitate transactions unless any concerns of potentially suspicious activity are resolved to their satisfaction.

3. Regulation J

61. The FRB's Regulation J "provides the legal framework for depository institutions to collect checks and other items and to settle balances through the Federal Reserve System" by specifying the "terms and conditions under which Federal Reserve Banks will receive items for collection from and present items to depository institutions."[132] Subpart B of Regulation J sets forth the FRB's rules and regulations for domestic wires sent through its Fedwire system, and incorporates Article 4A of the U.C.C., which applies to funds transfers.[133] Article 4A of the U.C.C., among other things, provides for the cancellation of funds transfers by their sending bank under certain conditions.[134]

---

130 USA PATRIOT Act, § 314.

131 USA PATRIOT Act, §§ 314(a) and 314(b).

132 "Regulation J: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers through Fedwire," Compliance Guide to Small Entities, Board of Governors of the Federal Reserve System, December 28, 2016, available at https://www.federalreserve.gov/supervisionreg/regjcg.htm, accessed February 5, 2021.

133 Title 12 of the Code of Federal Regulations ("12 C.F.R."), Part 210, Subpart B.

134 12 C.F.R. Part 210, Subpart B, Appendix B, at Section 4A-211(f).

62. My experience in banking supervision and compliance is that banks recognize that their BSA/AML obligations are not relieved by Regulation J's provisions, which govern the mechanics of funds transfers. Regulation J standardizes the funds-transfer process over the Fedwire system, and is not understood by banks and their regulators as having eased decades of BSA/AML laws and regulations enacted both before and after Regulation J. To the contrary, it is understood within the banking industry that Regulation J must be applied consistent with the intent and purpose of BSA/AML regulations, which have been strengthened over time, including with respect to wire transfers, as discussed above. In my experience, Regulation J is not understood to require banks to ignore their obligations to monitor and prevent potentially suspicious transactions and activities.

63. Accordingly, where Regulation J applies to a Fedwire payment, it is common practice for the bank that anticipates or accepts a wire transfer for the benefit of one of its customers to conduct due diligence and to request more information from the parties involved as necessary. Once a bank has identified a Fedwire payment as potentially suspicious, it is reasonable and consistent with industry standards and practices for the bank to apply additional scrutiny to the transaction, and potentially to return the wire transfer to the sending bank. Under those circumstances, a bank that facilitates the completion of the wire transfer and the beneficiary's withdrawal of funds does so contrary to industry practice. The common understanding in the banking industry is that BSA/AML regulations, the USA PATRIOT Act, FinCEN guidance, Regulation J and the U.C.C., and other laws and regulations governing wire transfers require the maintenance of safety and soundness in the banking system.

B. Banks' Internal Controls Are Designed to Ensure Compliance with Federal Banking Laws and Regulations

64. To comply with each of the laws and regulations described above, banks such as Chain Bridge develop internal documents such as policies and procedures and a code of conduct that they adhere to when conducting business. Each of these internal controls provides guidelines and processes that bank employees follow to ensure compliance with laws and regulations. During the relevant period, Chain Bridge had in place a code of conduct, as well as policies and procedures related to its BSA/AML program, wire transfer activity within its accounts, and the availability of funds within its accounts.[135] I describe each of these below.

65. Chain Bridge's policies and procedures for its BSA/AML program are outlined in its BSA, AML, and OFAC Policy.[136] The policy "establishes clear policies, procedures and internal controls" to minimize risk, identify and prevent potentially suspicious activities, and "comply with the requirements of the [BSA] and other related regulations issued by the Treasury Department, the Securities and Exchange Commission (SEC), and regulatory agencies."[137] The policy's guidelines and processes include, but are not limited to, identifying and responding to account activity that is potentially suspicious in nature.[138] Specifically, the policy identifies "certain

---

135 *See, e.g.*, Code of Conduct, Chain Bridge Bank, N.A., CBB00004363 - 379; Bank Secrecy Act, Anti Money Laundering Control, and Office of Foreign Assets Control Policy, Chain Bridge Bank, N.A., March 2020, CBB00004235 - 273; Wire Transfer Policy, Chain Bridge Bank, N.A., January 2020, CBB00004294 - 301; Funds Availability (Regulation CC) Policy, Chain Bridge Bank, N.A., January 2018, CBB00004307; Wire Transfer Procedures, Chain Bridge Bank, N.A., CBB00004302 - 306; Suspicious Activities Procedures, Chain Bridge Bank, N.A., September 2016, CBB00004274 - 276.

136 Bank Secrecy Act, Anti Money Laundering Control, and Office of Foreign Assets Control Policy, Chain Bridge Bank, N.A., March 2020, CBB00004235 - 273.

137 Bank Secrecy Act, Anti Money Laundering Control, and Office of Foreign Assets Control Policy, Chain Bridge Bank, N.A., March 2020, CBB00004235 - 273 at 236.

138 Bank Secrecy Act, Anti Money Laundering Control, and Office of Foreign Assets Control Policy, Chain Bridge Bank, N.A., March 2020, CBB00004235 - 273.

activities that are suspicious in nature and which shall alert the Bank as to the potential for the customer to conduct illegal activities at the institution," including:

i. "Insufficient, false, or suspicious information provided by the customer;"

ii. "Wire transfer activity which is not consistent with the business activities of the customer;" and

iii. "Funds transfers to foreign countries."[139]

66. Chain Bridge's Suspicious Activity Procedures provide further detail on the Bank's practices for responding to potentially suspicious activity.[140] The procedures note that "[w]ell informed employees are the first line of defense in preventing, identifying, and reporting money laundering and suspicious activity."[141] Consistent with industry standards and practices, Chain Bridge's Suspicious Activity Procedures identify examples of potentially suspicious activity that include, but are not limited to, 1) customers that are "reluctant to provide any information requested for proper identification," 2) deposits and immediate transfers of funds where such activity is "inconsistent with the customer's stated business," and 3) international funds transfers where the customer had "no history of such transfers."[142]

---

139 Bank Secrecy Act, Anti Money Laundering Control, and Office of Foreign Assets Control Policy, Chain Bridge Bank, N.A., March 2020, CBB00004235 - 273 at 246.

140 Suspicious Activities Procedures, Chain Bridge Bank, N.A., September 2016, CBB00004274 - 276.

141 Suspicious Activities Procedures, Chain Bridge Bank, N.A., September 2016, CBB00004274 - 276 at 274.

142 Suspicious Activities Procedures, Chain Bridge Bank, N.A., September 2016, CBB00004274 - 246 at 274 - 275. In addition, on September 12, 2019, Chain Bridge conducted training on Questionable and Suspicious Activity Reporting that detailed examples of such activity. *See* "BSA Policy Review: Questionable and Suspicious Activity Reporting (BSA Policy Pages 32 - 35)," BSA Training – BSA Policy Review, Chain Bridge Bank, N.A., September 12, 2019, CBB00004277 - 278.

67. The Bank outlines additional requirements related to wire transfer activity in its Funds Availability (Reg CC) Policy.[143] This policy states that for accounts less than 30 days old, funds received by wire transfer will be available only one business day after the deposit is completed.[144] This policy is frequently used in the banking industry to protect against potentially problematic movements of funds by new accounts before sufficient account history and other diligence has occurred, thereby providing a bank comfort in such transactions.

68. Chain Bridge's Code of Conduct further emphasizes the requirements outlined in the Bank's policies and procedures. It requires Bank personnel to "comply with all applicable laws, regulations, and Bank policies," including laws and regulations surrounding suspicious activity reporting and the USA PATRIOT Act, and the requirements outlined in the Bank's BSA, AML, and OFAC Policy.[145]

C. Federal Banking Laws and Regulations Have Taken on Heightened Importance During the COVID-19 Crisis

69. The COVID-19 pandemic, declared a public health crisis in mid-March of 2020, has given rise to unique challenges for U.S. financial institutions.[146] The containment measures adopted in response to these public health concerns have created operational challenges and

---

143 Wire Transfer Policy, Chain Bridge Bank, N.A., January 2020, CBB00004294 - 301; Funds Availability (Regulation CC) Policy, Chain Bridge Bank, N.A., January 2018, CBB00004307 - 309.

144 Funds Availability (Regulation CC) Policy, Chain Bridge Bank, N.A., January 2018, CBB00004307 - 309 at 309; Evinger Deposition, pp. 234:16 - 18 ("[T]he funds availability policy wouldn't have permitted us to provide . . . funds until the next business day"); Funds Availability Disclosure, Chain Bridge Bank N.A., CBB00002609 - 610 at 610 (relaying "Special Rules for New Accounts" to customers).

145 Code of Conduct, Chain Bridge Bank, N.A., CBB00004363 - 379 at 364 and 373 - 374.

146 "Proclamation 9994 of March 13, 2020: Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak," 85 Fed. Reg. 15337 (March 18, 2020), available at https://www.federalregister.gov/documents/2020/03/18/2020-05794/declaring-a-national-emergency-concerning-the-novel-coronavirus-disease-covid-19-outbreak, accessed February 5, 2021.

increased risk.[147] In addition, the demand for COVID-19-related health supplies and services such as masks has resulted in increased fraudulent transactions in the rush to protect public health.[148] As further explained below, federal regulators have responded by issuing news releases and regulatory guidance for financial institutions that emphasize the importance of federal banking laws and regulations, particularly those covering fraud prevention such as BSA/AML regulations and the USA PATRIOT Act.

70. **Exhibit 1** lists examples of news releases and regulatory guidance issued by law enforcement and regulatory entities on fraudulent activity during the COVID-19 pandemic. Some of these news releases and regulatory guidance are described in the paragraphs below.

71. On March 16, 2020, ten days before the California Wire Transfer, FinCEN published a news release advising U.S. financial institutions to "remain alert about malicious or fraudulent transactions similar to those that occur in the wake of natural disasters."[149] The news release detailed that the agency was "monitoring public reports and BSA reports of potential illicit

[147] "Interagency Examiner Guidance for Assessing Safety and Soundness Considering the Effect of the COVID-19 Pandemic on Financial Institutions," Federal Deposit Insurance Corporation, June 23, 2020, available at https://www.fdic.gov/news/financial-institution-letters/2020/fil20064.html, accessed February 5, 2021; "Interagency Examiner Guidance for Assessing Safety and Soundness Considering the Effect of the COVID-19 Pandemic on Institutions," Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, National Credit Union Administration, and State Financial Regulators, June 2020, available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20200623a1.pdf, accessed February 5, 2021.

[148] "FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic," Federal Bureau of Investigation, April 13, 2020, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic, accessed February 11, 2021; "The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity," Financial Crimes Enforcement Network, March 16, 2020, available at https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions, accessed February 5, 2021.

[149] "The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity," Financial Crimes Enforcement Network, March 16, 2020, available at https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions, accessed February 5, 2021.

behavior connected to COVID-19," including "[i]mposter scams," "[i]nvestment scams," and "[p]roduct scams."[150]

72. Two days later, on March 18, 2020, the U.S. Attorney for the Eastern District of Virginia warned of "supply scams" that "claim[] to sell medical supplies currently in high demand, such as surgical masks," and urged the public to "[b]e wary of any business … requesting payments … by wire transfer" and to avoid "send[ing] money through any of these channels."[151]

73. On March 25, 2020, the day before the California Wire Transfer, FFIEC members published a news release detailing that it was "actively discussing and identifying appropriate measures, both collaboratively and individually, to maintain safety and soundness [of U.S. financial institutions] while protecting consumers."[152]

74. As detailed in **Exhibit 1**, regulatory guidance related to financial transactions during the COVID-19 pandemic continued to be issued after the California Wire Transfer, with numerous regulatory entities issuing or updating their prior news releases.[153] In one notable example, FinCEN updated its guidance in May 2020 to inform banks that "[d]etecting, preventing,

---

[150] "The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity," Financial Crimes Enforcement Network, March 16, 2020, available at https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions, accessed February 5, 2021.

[151] "U.S. Attorney Warns of Coronavirus Scams Targeting Vulnerable Victims," The United States Attorney's Office for the Eastern District of Virginia, March 18, 2020, available at https://www.justice.gov/usao-edva/pr/us-attorney-warns-coronavirus-scams-targeting-vulnerable-victims, accessed February 5, 2021.

[152] "Financial Regulators Highlight Coordination and Collaboration of Efforts to Address COVID-19," Federal Financial Institutions Examination Council, March 25, 2020, available at https://www.ncua.gov/newsroom/press-release/2020/financial-regulators-highlight-coordination-and-collaboration-efforts-address-covid-19, accessed February 5, 2021.

[153] *See, e.g.*, "The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic," Financial Crimes Enforcement Network, April 3, 2020, available at https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial, accessed February 5, 2021.

and reporting" COVID-19 related scams "is critical to our national security."[154] The FBI also issued a warning about "rapidly emerging fraud trends" related to PPE procurement perpetrated specifically against "state government agencies."[155] Although this regulatory guidance was released after the events at issue, it reflects the specific application of pre-existing laws and regulations that ensure the safety and soundness of the banking system. It also reflects the type of prudence banks themselves were exercising prior to these specific issuances of regulatory guidance. That is, none of the aforementioned regulatory guidance pertained to newly-developed regulations; it was instead a reminder of the safety-and-soundness principles standard to the banking industry.[156]

VI. THE BLUE FLAME TRANSACTION AND CALIFORNIA WIRE TRANSFER EXHIBITED CHARACTERISTICS OF POTENTIALLY SUSPICIOUS AND CONCERNING ACTIVITY UNDER BSA/AML REGULATIONS AND INDUSTRY PRACTICES

75. In this section, I build upon the background presented in Section IV and Section V to evaluate the characteristics of the Blue Flame Transaction and California Wire Transfer. As I explained in Section V.A and V.B, federal regulators' objective of safety and soundness, BSA/AML and other regulations, and Chain Bridge's internal policies and procedures provide

---

154 "Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)," Financial Crimes Enforcement Network FIN-2020-A002, May 18, 2020, p. 1, available at https://www.fincen.gov/sites/default/files/advisory/2020-05-18/Advisory%20Medical%20Fraud%20Covid%2019%20FINAL%20508.pdf, accessed February 5, 2021.

155 "FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic," Federal Bureau of Investigation, April 13, 2020, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic, accessed February 11, 2021.

156 *See, e.g.*, "Advisories/Notices/Bulletins/Fact Sheets," Financial Crimes Enforcement Network, available at https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets, accessed February 5, 2021 (discussing the publication of advisories for banks to "enhance their [AML] monitoring systems for more valuable suspicious activity reporting").

guidance on managing risk in the banking system and identifying potentially suspicious account activity. This account monitoring has taken heightened importance during the COVID-19 pandemic.[157] As detailed in the sections below, based on my experience with banks' application of and adherence to the aforementioned laws and regulations, as well as my review of Chain Bridge's policies and procedures, the Blue Flame Transaction and California Wire Transfer exhibited characteristics of potentially suspicious and concerning activity. These circumstances, in my experience, would have given Chain Bridge reasonable doubt concerning whether Blue Flame Medical had a right to the payment sent by the State of California:

a. Blue Flame Medical was a newly formed entity with a new account and principals who were unable to furnish requested documentation, which did not provide Chain Bridge personnel with a sufficient understanding of the Blue Flame Transaction before the California Wire Transfer occurred;

b. The California Wire Transfer was substantially outside the initially disclosed and expected activity for Blue Flame Medical's account, and was notably larger than the transactions at Chain Bridge;

c. Based on information available to the Bank at the time of the California Wire Transfer, Blue Flame Medical and its founders had no prior experience with transactions similar to the Blue Flame Transaction or funds transfers similar to the California Wire Transfer;

d. Blue Flame Medical's principals and employees exhibited unusual and suspicious behaviors in their interactions with Chain Bridge personnel;

157 *See* Section V.C.

e. The Blue Flame Transaction was a "high velocity" transaction in which funds would be wired out of Blue Flame Medical's account a very short time after having been wired in;

f. The Blue Flame Transaction involved a high-risk jurisdiction and a stated business purpose related to a market known to have stressed business conditions at the time; and,

g. JPMorgan informed Chain Bridge that it had "concerns of fraud" regarding the California Wire Transfer, which was under review by JPMorgan's Global Securities Investigation Team.

A. Blue Flame Medical Was a Newly Formed Entity with a New Account and Principals Who Were Unable to Furnish Requested Documentation

76. The California Wire Transfer, which amounted to nearly $456.9 million, was received for the benefit of Blue Flame Medical only a day after the company's account was opened at Chain Bridge, and only three days after the company was formed. Indeed, when Mr. Gula informed Chain Bridge personnel about the incoming wire and its size, mid-afternoon on March 25, he advised that the wire's arrival was imminent (even though Blue Flame Medical's account had only been opened that morning).[158] Based on my experience, such circumstances are highly unusual within the banking industry and warranted further scrutiny by Chain Bridge.

77. Generally, a bank such as Chain Bridge follows a series of steps when opening accounts, including new account due diligence, in order to ensure compliance with laws and regulations and with the bank's internal controls.[159] In addition, based on my experience, when an

---

158 Call between Heather Schoeppe and Michael Gula, March 25, 2020, 3:27 p.m. ET, CBB00002794.

159 *See, e.g.*, "Customer Identification Program — Overview," BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. 47, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021; Bank

account holder expects to send or receive a large wire transfer outside of the account's expected activity, it is customary for the account holder to inform the bank sufficiently in advance, thereby providing the bank with enough time to prepare and conduct any necessary due diligence on the transaction.[160] Any large transaction outside the account's expected activity for which the bank receives little advance notice would merit further scrutiny by the bank.[161]

78. When Mr. Brough and Mr. Evinger asked for additional documentation regarding the Blue Flame Transaction, the information provided was inconsistent with their requests.[162] Mr. Evinger testified that the "copies of the contracts" with the State of California and with Mr. Gula's manufacturer were "an important part of [Chain Bridge's] due diligence."[163] However, Mr. Evinger explained that the email screenshot and website link provided by Mr. Gula did not satisfy his request for the underlying documentation on the Blue Flame Transaction.[164] This indicated that Chain Bridge personnel did not have a sufficient understanding of the Blue Flame Transaction

Secrecy Act, Anti Money Laundering Control, and Office of Foreign Assets Control Policy, Chain Bridge Bank, N.A., March 2020, CBB00004235 - 273 at 258 - 266.

160 *See, e.g.*, Bank Secrecy Act, Anti Money Laundering Control, and Office of Foreign Assets Control Policy, Chain Bridge Bank, N.A., March 2020, CBB00004235 - 273 at 256 - 258.

161 *See, e.g.*, "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, pp. F-2, F-8, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021; Bank Secrecy Act, Anti Money Laundering Control, and Office of Foreign Assets Control Policy, Chain Bridge Bank, N.A., March 2020, CBB00004235 - 273 at 244 - 245 and 267.

162 Email from Michael Gula to Brielle Appelbaum, "Fwd: My memory of the call with Chain Bridge Bank," May 9, 2020, BFM000137279 - 280; Emails between John Brough, David Evinger, and Michael Gula, "Contact Info," March 25, 2020, BFM000013445 - 447 at 445 - 446; Wiring Instructions from Great Health Companion Group Ltd. Co. for Beneficiary Wingar Industrial Inc., BFM000013448; Email from Michael Gula to David Evinger and John Brough, "Screenshot 2020-03-25 at 6.26.08 PM," March 25, 2020, CBB00002699; Screenshot sent by Michael Gula to David Evinger and John Brough, March 25, 2020, CBB00002700; Email from Mike Gula to David Evinger. "Blue Flame Medical | Fighting Coronavirus," March 26, 2020, CBB00002686; Evinger Deposition, pp. 202:4 - 13, 222:8 - 223:8.

163 Evinger Deposition, pp. 202:10 - 13, 222:13 - 223:3.

164 Evinger Deposition, pp. 222:8 - 223:8, 228:17 - 19. *See also* Brough Deposition, p. 355:16 - 17 ("Mr. Gula never supplied the requested information").

before the California Wire Transfer occurred, and were seeking documentation that could provide them with such an understanding.

79. Furthermore, the California Wire Transfer was executed within such a short amount of time after Blue Flame Medical's account opening that the full set of account-opening documents had not been completed by the time the wire transfer came through. In particular, the Account Agreement was never signed by Mr. Thomas, and was signed by Mr. Gula before the Bank received Blue Flame Medical's articles of incorporation and EIN to verify the corporation's identity.[165] In addition, the account's online functionality to send outgoing wires was not yet set up at the time the California Wire Transfer came through, though Mr. Gula insisted that any funds received would need to be wired out immediately.[166]

80. BSA/AML regulations note that when a business is "reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business [or] anticipated account activity," it is considered a potentially suspicious activity that may merit additional scrutiny.[167] BSA/AML regulations also warn of "payments or receipts with no apparent links to legitimate contracts, goods, or services."[168]

---

[165] Account Agreement between Chain Bridge Bank, N.A. and Blue Flame Medical LLC, March 25, 2020, CBB00000555 - 556; Email from Michael Gula to Mariano Castagnello, "Fwd: need BF Medical EIN/registration," March 25, 2020, CBB00002563 - 564; Notification of Employer Identification Number for Blue Flame Medical LLC, Internal Revenue Service, March 24, 2020, CBB00002565 - 567; State of Delaware Limited Liability Company Certificate of Formation for Blue Flame Medical LLC, March 23, 2020, CBB00002569 - 571.

[166] Emails between Maria Cole and Michael Gula, "RE: NEW business account needed," March 25, 2020, CBB00001514 - 517 at 514 - 515. Ms. Cole sent a Wire Transfer Request Form to Mr. Gula and Mr. Thomas on March 26 at 12:10 p.m. *See* Email from Maria Cole to John Thomas, cc'ing Michael Gula and Mike Richardson, "Wire Request Form," March 26, 2020, BFM000111337.

[167] "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. F-1, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

[168] "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. F-3, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

81. Additionally, FinCEN guidance related to medical supply scams warns that "[f]inancial indicators of these scams may include … [a] newly-opened account [that] receives a large wire transaction that the accountholder failed to mention during the account opening process" and a merchant that "cannot explain the source of the goods or how the merchant acquired bulk supplies of highly sought-after goods related to the COVID-19 pandemic."[169] Other FinCEN red flags include when a seller is "reluctant to provide … the financial institution that is processing the transactions with invoices or other documentation supporting the stated purpose" of the transaction, and when a financial institution "does not understand the merchant's business model" or "has difficulty determining the true nature of the company and its operations."[170]

82. FBI guidance on suspicious activity related to the COVID-19 pandemic also warns of transactions where "a seller or broker cannot clearly explain the origin of the items or how they are available given current demand," where "a seller or broker is not an entity with which the buyer has an existing business relationship," and where there is "[u]nexplained urgency to transfer funds."[171]

83. The undisclosed nature of the California Wire Transfer at account opening and Mr. Gula's inability to furnish the requested documentation for the Blue Flame Transaction, including

---

169 "Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)," Financial Crimes Enforcement Network FIN-2020-A002, May 18, 2020, pp. 4-5, available at https://www.fincen.gov/sites/default/files/advisory/2020-05-18/Advisory%20Medical%20Fraud%20Covid%2019%20FINAL%20508.pdf, accessed February 5, 2021.

170 "Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)," Financial Crimes Enforcement Network FIN-2020-A002, May 18, 2020, p. 4, available at https://www.fincen.gov/sites/default/files/advisory/2020-05-18/Advisory%20Medical%20Fraud%20Covid%2019%20FINAL%20508.pdf, accessed February 5, 2021.

171 "FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic," Federal Bureau of Investigation, April 13, 2020, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic, accessed February 11, 2021.

the underlying contracts, were characteristics of potentially suspicious and concerning activity, both in general and specifically related to transactions during the COVID-19 pandemic.

B. The California Wire Transfer Was Substantially Outside the Initially Disclosed and Expected Activity for Blue Flame Medical's Account, and Was Notably Larger than Previous Wire Transfers at Chain Bridge

84. At nearly $456.9 million, the California Wire Transfer was substantially larger than what Mr. Gula had stated at account opening for Blue Flame Medical's expected account activity, which is a characteristic of potentially suspicious and concerning activity under BSA/AML regulations and industry practices. The wire transfer was also notably larger than previous wire transfers at Chain Bridge.

85. When Mr. Gula opened Blue Flame Medical's account, he represented to Mr. Castagnello that incoming wire transfers would total an average of $100 million per month ($25 million across five foreign wire transfers, and $75 million across 25 domestic wire transfers).[172] Only later that day, and after obtaining wire instructions for the new account, did Mr. Gula inform Chain Bridge personnel that he expected a $450 million dollar wire transfer to be received as soon as that same day, the amount of which was substantially different from the account activity he represented only a few hours earlier at account opening.[173] The $456.9 million California Wire Transfer that arrived the next day was nearly five times greater than what Mr. Gula had described

[172] Call between Heather Schoeppe and Michael Gula, March 25, 2020, 3:27 p.m. ET, CBB00002794; Call between Heather Schoeppe and Joanna Williamson, March 25, 2020, 4:25 p.m. ET, CBB00002797; Schoeppe Deposition, pp. 137:8 - 138:1 (identifying the call as the "first time" Ms. Schoeppe became aware of the amount of the wire); Email from Mariano Castagnello to Tsega Yohannes, "RE: Expected activity," March 27, 2020, CBB00001202 - 203.

[173] *See, e.g.*, Email from Maria Cole to Michael Gula, "RE: wire," March 26, 2020, CBB00001781 - 782 at 781; "Instructions for wiring funds to Chain Bridge Bank, N.A.," CBB00001784; Email from Heather Schoeppe to Mike Richardson, John Brough, and Joanna Williamson, "FW: Blue Flame Medical incoming wire 450 million," March 25, 2020, CBB00000686 - 695 at 693 - 694; Email from Michael Gula to David Evinger, cc'ing John Brough, "RE: Contact Info," March 25, 2020, BFM000074101 - 106 at 104.

just hours earlier as the account's average monthly wire transfer activity. In addition, I understand that it was twenty-two times larger than the largest wire transfer previously received by Chain Bridge.[174]

86. Relatedly, around the same time that Chain Bridge received the California Wire Transfer, the Bank received outgoing wire instructions from Ethan Bearman, a person whose name was not associated with Blue Flame Medical's account documents.[175] Mr. Bearman requested that the Bank send an outgoing wire to Suuchi Inc., yet Mr. Gula represented to Mr. Brough and Mr. Evinger the previous evening that outgoing wires would be sent to Wingar Industrial Inc.[176] Although Mr. Thomas followed up to introduce Mr. Bearman as Blue Flame Medical's counsel, the receipt of inconsistent outgoing wire instructions from an unknown source would have reasonably raised additional concern among Bank personnel.[177]

87. BSA/AML regulations note that when "funds transfer activity … shows unusual patterns," it may be considered potentially suspicious activity that merits additional scrutiny.[178] A transaction of this size, which was (i) outside the expectations for Blue Flame Medical; (ii) outside the norm for Chain Bridge; (iii) first disclosed by Blue Flame Medical mere hours after its account

[174] Brough Deposition, p. 351:2 - 9.

[175] Email from John Thomas to Ethan Bearman, cc'ing Maria Cole and Michael Gula, "Re: Blue Flame Medical LLC-Wire Transfer," March 26, 2020, CBB00000655 - 657 at 656; Account Agreement between Chain Bridge Bank, N.A. and Blue Flame Medical LLC, March 25, 2020, CBB00000555 - 556.

[176] Email from John Thomas to Ethan Bearman, cc'ing Maria Cole and Michael Gula, "Re: Blue Flame Medical LLC-Wire Transfer," March 26, 2020, CBB00000655 - 657 at 656; Emails between John Brough, David Evinger, and Michael Gula, "Contact Info," March 25, 2020, BFM000013445 - 447 at 445; Wiring Instructions from Great Health Companion Group Ltd. Co. for Beneficiary Wingar Industrial Inc., BFM000013448.

[177] Email from John Thomas to Ethan Bearman, cc'ing Maria Cole and Michael Gula, "Re: Blue Flame Medical LLC-Wire Transfer," March 26, 2020, CBB00000655 - 657 at 656.

[178] "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. F-2, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

opening; and (iv) followed by outgoing wire instructions that were inconsistent with information previously provided, was characteristic of potentially suspicious and concerning activity.

C. Blue Flame Medical and Its Founders Had No Prior Experience with Transactions Similar to the Blue Flame Transaction or Funds Transfers Similar to the California Wire Transfer

88. Based on the information produced in this matter and available to the Bank at the time of the California Wire Transfer, Blue Flame Medical's founders, Mr. Gula and Mr. Thomas, had no prior experience in procuring and distributing PPE, and had not engaged in transactions of any type that were similar in size to the Blue Flame Transaction.[179] This lack of prior experience indicates potentially suspicious and concerning activity under BSA/AML regulations, industry practices, and Chain Bridge's own policies and procedures.

89. In an internal email, Ms. Schoeppe stated that Mr. Brough and Mr. Evinger "are very skeptical about [the Blue Flame Transaction] ... [t]hey just think it seems very strange a company established 2 days ago would get awarded this huge contract from California."[180] During his call with Mr. Brough and Mr. Evinger, Mr. Gula conveyed that he understood it was hard for the Bank to believe that he could transition from a business with annual deposits in hundreds of thousands of dollars to one with transactions in hundreds of millions.[181] Mr. Brough and Mr. Evinger also testified that the State of California sounded "surprised" to learn of Mr. Gula's and

[179] Complaint, ¶ 22; Blue Flame Medical Presentation, BFM000002416 - 430 at 419 - 420; Gula Deposition, p. 25:6 - 18; Thomas Deposition, p. 19:17 - 19; Email from Michael Gula to Brielle Appelbaum, "Fwd: My memory of the call with Chain Bridge Bank," May 9, 2020, BFM000137279 - 280.

[180] Email from Heather Schoeppe to Mike Richardson, "Re: Blue Flame Medical incoming wire 450 million," March 25, 2020, CBB00000686 - 695 at 692.

[181] Email from Michael Gula to Brielle Appelbaum, "Fwd: My memory of the call with Chain Bridge Bank," May 9, 2020, BFM000137279 - 280.

Mr. Thomas's lack of experience and the newness of Blue Flame Medical and its account at Chain Bridge.[182]

90. Although Mr. Gula had been a Chain Bridge customer for more than a decade, with both personal and other business accounts at the Bank, a nearly $456.9 million wire transfer was unusual activity for Mr. Gula's accounts more generally.[183] Considering the California Wire Transfer in the context of Mr. Gula's historical transaction activity, it was unusual enough to be characterized as potentially suspicious and concerning activity.

91. In addition, Blue Flame Medical was affiliated with Blue Flame Strategies and Redline Strategies, which were also entities newly formed by Mr. Gula and Mr. Thomas, with accounts that had been opened at Chain Bridge less than two weeks prior.[184]

92. BSA/AML regulations state that transactions where the "customer's background differs from that which would be expected on the basis of his or her business activities" or that are "high-value" and "not commensurate with the customer's known incomes" are potentially suspicious activities that may warrant additional scrutiny.[185] Similarly, FBI guidance on suspicious activity related to the COVID-19 pandemic warns of transactions where potential buyers "cannot verify with the product manufacturer that the seller is a legitimate distributor," and where "[t]he

---

182 Evinger Deposition, p. 282:10 - 14; Brough Deposition, p. 283:9 - 21.

183 Complaint, ¶ 27; Email from Michael Gula to Brielle Appelbaum, "Fwd: My memory of the call with Chain Bridge Bank," May 9, 2020, BFM000137279 - 280; Call between Rakesh Korpal, David Evinger, and John Brough, 12:44 p.m. ET, CBB00002541.

184 State of Delaware Limited Liability Company Certificate of Formation for Blue Flame Strategies LLC, February 10, 2020, CBB00001198 - 199; State of Delaware Limited Liability Company Certificate of Formation for Redline Strategies LLC, March 16, 2020, CBB00001577 - 579; Account Agreement between Chain Bridge Bank, N.A. and Blue Flame Strategies LLC, March 16, 2020, CBB00004391 - 392; Account Agreement between Chain Bridge Bank, N.A. and Redline Strategies LLC, March 18, 2020, CBB00004380 - 381.

185 "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, pp. F-1 and F-8, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

seller or broker is not an entity with which the buyer has an existing business relationship."[186] BSA/AML regulations also warn that customers with "established multiple accounts in various corporate or individual names that lack sufficient business purpose for the account complexities" may merit additional scrutiny.[187] In this instance, Chain Bridge was aware that Blue Flame Medical and its principals had no prior experience in the field of PPE supply, no history of transactions similar to the Blue Flame Transaction, and no history of any funds transfers similar to the California Wire Transfer. Each of these is characteristic of potentially suspicious and concerning activity under BSA/AML regulations and industry practices.

D. Blue Flame Medical's Principals and Employees Exhibited Unusual and Suspicious Behaviors in Their Interactions with Chain Bridge Personnel

93. On March 25, 2020, Chain Bridge's branch office was closed to customers due to COVID-19 quarantine procedures and Bank personnel were directing customers to conduct any account activity online.[188] Mr. Gula had recently opened checking accounts for Blue Flame Strategies and Redline Strategies via online communications with Ms. Cole, but opened the Blue

[186] "FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic," Federal Bureau of Investigation, April 13, 2020, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic, accessed February 11, 2021.

[187] "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. F-8, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

[188] Evinger Deposition, pp. 129:19 - 130:6.

Flame Medical account in person.[189] According to contemporaneous statements from Bank personnel, Mr. Gula was "panicked and … pushing [Chain Bridge] to open an account."[190]

94. During his deposition, Mr. Brough recalled that on his March 25 call with Mr. Gula, Mr. Gula stated that the Blue Flame Transaction would be his "payday," and that he wanted to "get out" from his political profession.[191] Mr. Evinger also recalled that Mr. Gula stated he was planning to "leave this all behind" and "make enough money to never have to worry about anything."[192]

95. In the hours before and after the wire transfer was received by Chain Bridge, Mr. Gula, Mr. Thomas, and Mr. Bearman emailed and called the Bank numerous times to check on the status of the California Wire Transfer and inquire as to when money could be wired out.[193] Chain Bridge personnel noted in internal communications that Mr. Gula "is calling us so much" and "is extremely aggressive and will not hang up."[194]

---

[189] Email from Michael Gula to Melissa Strano, cc'ing John Thomas, "Fwd: new business," March 13, 2020, CBB00001952; Email from Maria Cole to Michael Gula, cc'ing Mariano Castagnello, Mike Richardson, and Brad Ward, "New Account," March 16, 2020, CBB00001191 - 192; Email from Michael Gula to Maria Cole, cc'ing John Thomas, "NEW business account needed," March 17, 2020, CBB00001574; Defendants' Responses to Plaintiff's First Set of Interrogatories, October 28, 2020, Response to Interrogatory No. 2, p. 3; Evinger Deposition, pp. 129:19 - 130:12; Call between Heather Schoeppe and Mike Richardson, March 25, 2020, 9:23 a.m. ET, CBB00002792.

[190] Call between Heather Schoeppe and Joanna Williamson, March 25, 2020, 4:25 p.m. ET, CBB00002797; Schoeppe Deposition, p. 46:11 - 21.

[191] Brough Deposition, pp. 346:11 - 350:3.

[192] Evinger Typed Notes, CBB00004453 - 462 at 454.

[193] *See, e.g.*, Emails between Mike Richardson and Maria Cole, cc'ing Heather Schoeppe, "Re: Blue Flame Medical incoming wire 450 million," March 25 - 26, 2020, CBB00000686 - 695 at 689; Email from John Thomas to Ethan Bearman, cc'ing Maria Cole and Michael Gula, "Re: Blue Flame Medical LLC- Wire Transfer," March 26, 2020, CBB00000655 - 657 at 656; Email from Heather Schoeppe to Thais Ribeiro, John Brough, David Evinger, and Mike Richardson, cc'ing Wires, "RE: Incoming Large Wire," March 26, 2020, CBB00000741 - 743 at 741 - 742; Call Log for Chain Bridge Bank, CBB00004323 - 362 at 348 - 349; Call between Maria Cole and John Thomas, March 26, 2020, 11:02 a.m. ET, CBB00002786; Call between Maria Cole and John Thomas, March 26, 2020, 11:51 a.m. ET, CBB00002787; Call between Maria Cole and John Thomas, March 26, 2020, 11:59 a.m. ET, CBB00002788.

[194] Email from Heather Schoeppe to Thais Ribeiro, John Brough, David Evinger, and Mike Richardson, cc'ing Wires, "RE: Incoming Large Wire," March 26, 2020, CBB00000741 - 743 at 741 - 742. *See also* Schoeppe Deposition, pp. 106:21 - 107:12, 248:16 - 249:3.

96. In addition, Mr. Gula and Mr. Thomas stated that they needed to know the moment the California Wire Transfer hit their account.[195] Similarly, during his calls with Ms. Cole, Mr. Thomas asked to have Chain Bridge personnel stay on the phone until the moment the wire was received, and described himself as a "ball of nerves."[196]

97. FBI guidance on suspicious activity related to COVID-19 pandemic warns of an "[u]nexplained urgency to transfer funds."[197] Mr. Gula's, Mr. Thomas's, and Mr. Bearman's insistent need to know the moment the wire transfer was received by the Bank and when it could be wired out, as well as Mr. Gula's and Mr. Thomas's unusual statements to Bank personnel, are characteristics of potentially suspicious and concerning activity.

E. The Blue Flame Transaction Was a "High Velocity" Transaction

98. Shortly after Blue Flame Medical's checking account was opened, Chain Bridge personnel, including Mr. Brough, learned from Mr. Gula that "the money [for the Blue Flame Transaction] should be in today and will be spent out fairly rapidly as China produces the masks and [Blue Flame Medical] pay[s] them."[198] Just as the California Wire Transfer was being received, moreover, Mr. Thomas "confidentially" disclosed to Ms. Cole that Blue Flame Medical planned to move "several billion dollars" through the account over the next few weeks.[199]

195 Call between Heather Schoeppe and Michael Gula, March 25, 2020, 3:27 p.m. ET, CBB00002794; Call between Maria Cole and John Thomas, March 26, 2020, 11:02 a.m. ET, CBB00002786; Call between Maria Cole and John Thomas, March 26, 2020, 11:51 a.m. ET, CBB00002787.

196 Call between Maria Cole and John Thomas, March 26, 2020, 11:02 a.m. ET, CBB00002786; Call between Maria Cole and John Thomas, March 26, 2020, 11:51 a.m. ET, CBB00002787.

197 "FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic," Federal Bureau of Investigation, April 13, 2020, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic, accessed February 11, 2021.

198 Email from Heather Schoeppe to Mike Richardson, John Brough, and Joanna Williamson, "FW: Blue Flame Medical incoming wire 450 million," March 25, 2020, CBB00000686 - 695 at 693 - 694.

199 Call between Maria Cole and John Thomas, March 26, 2020, 11:02 a.m. ET, CBB00002786.

99. Transactions such as those mentioned by Mr. Gula and Mr. Thomas are often referred to as a "high velocity" transactions because they involve funds that are wired into an account and then very quickly wired out.[200] Chain Bridge's own policies and procedures require employees to identify and investigate high velocity transactions.[201] Such high velocity transactions are characteristic of potentially suspicious and concerning activity under BSA/AML regulations and industry practices.

F. The Blue Flame Transaction Involved a High-Risk Jurisdiction and a Stated Business Purpose Related to a Market Known to Have Stressed Business Conditions at the Time

100. After Mr. Brough learned of the California Wire Transfer, he asked Mr. Gula if he had "sen[t] any money to China or others as a 'fee' for these transactions," to which Mr. Gula responded, "no, we have not sent the money to China but when we do[,] this is where we are sending it," attaching domestic wire instructions for Wingar Industrial Inc. with a header listing Great Health Companion Group, an entity that was ultimately owned by a Chinese SOE.[202] Although the outgoing wire was to a U.S. financial institution, Mr. Gula had made clear that its ultimate destination was China.[203] In addition, upon an Internet search of Wingar Industrial Inc., Mr. Evinger discovered that the company was a cutlery and flatware retailer.[204] BSA/AML

---

200 *See* "Appendix O: Examiner Tools for Transaction Testing," BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. O-3, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

201 Suspicious Activities Procedures, Chain Bridge Bank, N.A., September 2016, CBB00004274 - 276 at 275.

202 Emails between John Brough, David Evinger, and Michael Gula, "Contact Info," March 25, 2020, BFM000013445 - 447; Wiring Instructions from Great Health Companion Group Ltd. Co. for Beneficiary Wingar Industrial Inc., BFM000013448; Blue Flame Medical Presentation, BFM000002416 - 430 at 422.

203 Emails between John Brough, David Evinger, and Michael Gula, "Contact Info," March 25, 2020, BFM000013445 - 447 at 445; Wiring Instructions from Great Health Companion Group Ltd. Co. for Beneficiary Wingar Industrial Inc., BFM000013448; Call between Heather Schoeppe and Joanna Williamson, March 25, 2020, 4:25 p.m. ET, CBB00002797.

204 Brough Deposition, pp. 159:18 - 160:2; "Welcome," Wingar Industrial Inc., available at https://wingar.com/, accessed February 10, 2021.

regulations consider funds transfer activity with "unusual patterns" as well as business conducted in higher-risk jurisdictions (including China) to be potentially suspicious activities.[205] Chain Bridge's own policies and procedures also require employees to identify and investigate international transactions for accounts with no history of such transfers.[206]

101. The Blue Flame Transaction also involved a large quantity of PPE (100 million N95 masks) at the onset of the COVID-19 pandemic.[207] As explained in Section V.C. above, multiple regulatory entities warned of suspicious activity related to the COVID-19 pandemic, particularly surrounding medical supplies and masks. In particular, FinCEN guidance related to the COVID-pandemic identifies potentially suspicious circumstances as situations in which a financial institution "has difficulty determining the true nature of the company and its operations."[208] Mr. Evinger also testified that there was a concern for Mr. Gula and Blue Flame Medical to not be a "victim of something untoward."[209] That Blue Flame Medical planned to immediately wire large sums to a high-risk jurisdiction for products that were in high demand and for which regulatory entities warned of suspicious activity from suppliers are characteristics of potentially suspicious and concerning activity.

---

205 "Appendix F: Money Laundering and Terrorist Financing 'Red Flags,'" BSA/AML Manual, Federal Financial Institutions Examination Council, 2014, p. F-2, available at https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf, accessed February 5, 2021.

206 Suspicious Activities Procedures, Chain Bridge Bank, N.A., September 2016, CBB00004274 - 276 at 275.

207 Emails between John Thomas and Michael Wong, "Invoice," March 25, 2020, BFM000074110 - 111; Invoice from Blue Flame Medical LLC to Michael Wong, Contracts Administrator for State of California - General Services Procurement Division to Blue Flame Medical LLC, March 25, 2020, BFM000066431; Purchasing Authority Purchase Order from the State of California - General Services Procurement Division to Blue Flame Medical LLC, March 25, 2020, BFM000095501.

208 "Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)," Financial Crimes Enforcement Network FIN-2020-A002, May 18, 2020, p. 4, available at https://www.fincen.gov/sites/default/files/advisory/2020-05-18/Advisory%20Medical%20Fraud%20Covid%2019%20FINAL%20508.pdf, accessed February 5, 2021.

209 Evinger Deposition, p. 200:6 - 10.

G. JPMorgan Informed Chain Bridge That It Had "Concerns of Fraud" Regarding the California Wire Transfer, Which Was Under Review by JPMorgan's Global Securities Investigation Team

102. Approximately thirty minutes after Chain Bridge received the California Wire Transfer and before the Bank spoke with State of California officials knowledgeable about the Blue Flame Transaction, Mr. Coffey called Chain Bridge to place the funds on hold because JPMorgan had "concerns of fraud" regarding the transaction.[210] Mr. Coffey reported to Mr. Evinger that JPMorgan had suspicions regarding the California Wire Transfer and wanted Chain Bridge to hold the funds, to which Mr. Evinger responded that Chain Bridge had similar concerns and had already placed the funds on hold.[211] Shortly thereafter, Mr. Brough and Mr. Evinger learned from Mr. Korpal that the California Wire Transfer was flagged by JPMorgan's Global Securities Investigation Team, and that JPMorgan's research on the transaction was "all leading to not-good places."[212] Subsequently, Mr. Coffey called Mr. Evinger and Mr. Brough to inform them that JPMorgan "ha[s] enough concerns that we feel we need to claw those funds back."[213]

103. That JPMorgan (1) contacted Chain Bridge approximately thirty minutes after sending the California Wire Transfer to report its "concerns of fraud" and asked the Bank to hold the funds, (2) informed the Bank that the transaction was under investigation, and (3) ultimately reported that JPMorgan had enough concerns to recall the funds reflected another bank's apparent conclusion that the California Wire Transfer and Blue Flame Transaction exhibited characteristics of potentially suspicious and concerning activity under BSA/AML regulations and industry practices. In my experience, this highly unusual action was yet another indicator of potentially

---

[210] Coffey Deposition, p. 65:10 - 16; Call between Mariano Castagnello and Tim Coffey, March 26, 2020, 12:31p.m. ET, CBB00002784. *See also* Coffey Deposition, pp. 82:6 - 83:22 and Korpal Deposition, p. 222:17 - 22.

[211] Coffey Deposition, pp. 64:13 - 66:4.

[212] Call between David Evinger, John Brough and Rakesh Korpal, 12:44 p.m. ET, CBB00002541 - 542 at 541.

[213] Call between David Evinger, John Brough and Tim Coffey, 1:37 p.m. ET, CBB00002545.

suspicious and concerning activity, which occurred after Chain Bridge had received a myriad of other indicators.

VII. THE ACTIONS TAKEN BY CHAIN BRIDGE PERSONNEL AFTER OPENING BLUE FLAME MEDICAL'S CHECKING ACCOUNT AND RECEIVING THE CALIFORNIA WIRE TRANSFER WERE REASONABLE AND CONSISTENT WITH INDUSTRY STANDARDS AND PRACTICES

104. Based on my experience and my analysis of the facts and circumstances at issue in this matter, the decisions by Chain Bridge personnel to ask questions of the State of California regarding the California Wire Transfer, to honor JPMorgan's request to return the California Wire Transfer, and to close the Blue Flame Medical-related accounts were reasonable and consistent with industry standards and practices.

105. As a consultant to various financial institutions, I would not advise a bank on the basis of Regulation J to abstain from conducting due diligence if presented with the indicators of potentially suspicious activity that were present for the California Wire Transfer and Blue Flame Transaction. Nor would I advise a bank to make funds available to a wire transfer's beneficiary until concerns associated with those indicators of potentially suspicious activity—which could reveal illicit activity for which a bank could be held civilly or criminally liable for facilitating—had been resolved.

106. Each of the actions undertaken by Chain Bridge personnel is an example of Chain Bridge having effective internal controls and reflects the importance of the due diligence and transaction monitoring that banks undertake. The events that occurred during the first thirty hours that the Blue Flame Medical account was open provided Chain Bridge with sufficient reason to honor JPMorgan's request to return the California Wire Transfer.

VIII. CHAIN BRIDGE'S PLANNED USE OF AN ICS OR CDARS ACCOUNT REFLECTS COMMON INDUSTRY PRACTICE TO MAXIMIZE FDIC INSURANCE ON A LARGE DEPOSIT

107. I understand that Plaintiff in this matter has alleged that Chain Bridge returned the California Wire Transfer to JPMorgan not because of any concerns about potentially suspicious activity, but rather because the Bank was concerned that a $456.9 million deposit would trigger "additional capital reserve requirements."[214] I also understand that Plaintiff has argued that internal bank communications regarding the potential use of off-balance-sheet accounts to manage Blue Flame Medical's deposit provide evidence that Chain Bridge had concerns regarding various regulatory requirements.

108. In my experience, midsize banks such as Chain Bridge often have various reasons, unrelated to regulatory requirements, for assessing whether to move a portion of a large deposit off the bank's balance sheet. Those reasons may include the ability to maximize FDIC insurance on the deposit, and to provide the bank flexibility in its investment portfolio and management strategy.

109. For example, it is common for banks to use an ICS account to hold some or all of a large customer deposit off-balance-sheet in FDIC-insured accounts.[215] ICS accounts are a service developed by IntraFi Network to encourage competition between small, midsize, and large banks for large deposits.[216] Banks such as Chain Bridge rely on ICS accounts to insure large deposits that

---

[214] Complaint, ¶ 76.

[215] "How ICS and CDARS Work," ICS & CDARS, available at https://www.icsandcdars.com/how-it-works, accessed February 3, 2021; "IntraFi Network," ICS & CDARS, available at https://www.icsandcdars.com/about/intrafi-network-overview, accessed February 3, 2021.

[216] "IntraFi Network: Insured Cash Sweep Service, or ICS," American Bankers Association, available at https://www.aba.com/member-tools/industry-solutions/endorsed-solutions/promontory-interfinancial-network-insured-cash-sweep-service, accessed February 3, 2021.

exceed per-account FDIC-insurance limits at individual banks, which are normally set at $250,000.[217]

110. ICS accounts are widely used in the banking industry, and Chain Bridge's planned use of an ICS account to protect and manage a $456.9 million deposit is consistent with this common practice.[218] In my experience, the preparation of an ICS account for a deposit the size of the California Wire Transfer is consistent with responsible and sound banking practices. In addition, a bank's preparation to open an ICS account does not suggest that a large deposit imposes any additional regulatory requirements on the bank.

111. As explained in Section VI.B above, the California Wire Transfer amounted to nearly $456.9 million, and would result—if kept in Blue Flame Medical's account—in a large sum of Blue Flame Medical's funds at the Bank remaining uninsured by the FDIC.[219] It is therefore not surprising, and consistent with my experience and with industry practice, that Chain Bridge personnel began taking steps to open an ICS account for Blue Flame almost immediately after learning of the incoming California Wire Transfer. Such an account, once opened, would have facilitated FDIC insurance for more than $100 million of the California Wire Transfer.[220]

---

217 "How ICS and CDARS Work," ICS & CDARS, available at https://www.icsandcdars.com/how-it-works, accessed February 3, 2021; "IntraFi Network: Insured Cash Sweep Service, or ICS," American Bankers Association, available at https://www.aba.com/member-tools/industry-solutions/endorsed-solutions/promontory-interfinancial-network-insured-cash-sweep-service, accessed February 3, 2021.

218 "IntraFi Network," ICS & CDARS, available at https://www.icsandcdars.com/about/intrafi-network-overview, accessed February 3, 2021; "IntraFi Network: Insured Cash Sweep Service, or ICS," American Bankers Association, available at https://www.aba.com/member-tools/industry-solutions/endorsed-solutions/promontory-interfinancial-network-insured-cash-sweep-service, accessed February 3, 2021.

219 *See* "Deposit Insurance At a Glance," Federal Deposit Insurance Corporation, July 10, 2020, available at https://www.fdic.gov/resources/deposit-insurance/brochures/deposits-at-a-glance/, accessed February 3, 2021.

220 "IntraFi Network," ICS & CDARS, available at https://www.icsandcdars.com/about/intrafi-network-overview, accessed February 3, 2021; "How ICS and CDARS Work," ICS & CDARS, available at https://www.icsandcdars.com/how-it-works, accessed February 3, 2021; Brough Deposition, pp. 255:13 - 256:7.

112. Accordingly, shortly after receiving notice from Mr. Gula of the California Wire Transfer, Ms. Schoeppe alerted Ms. Williamson, who stated, "we'll do whatever we need to do," and asked if it would be possible to place some of the funds into an ICS account.[221] Mr. Brough and Mr. Evinger informed Mr. Gula and Mr. Case of their intention to rely on an ICS account to hold a portion of the California Wire Transfer's funds, and discussed setting up an ICS account with Chain Bridge personnel.[222] Mr. Richardson and Ms. Cole subsequently communicated through the next morning to prepare the ICS account paperwork so as to have it ready for Mr. Gula and Mr. Thomas to sign shortly after the Bank received notice that the California Wire Transfer had been received.[223] Such actions by the Bank are consistent with the common use of ICS accounts in the banking industry to accommodate large deposits.

113. The Bank also considered the use of a similar type of off-balance-sheet account, known as a CDARS account, which functions largely the same as an ICS account but invests funds in certificates of deposit rather than demand deposit or money market deposit accounts.[224] CDARS accounts also provide customers with FDIC insurance.[225] Had Chain Bridge deposited a portion of the California Wire Transfer into a CDARS account, its actions would have been consistent with the banking industry's common use of CDARS accounts to manage and insure large deposits. A

221 Call between Heather Schoeppe and Joanna Williamson, March 25, 2020, 4:25 p.m. ET, CBB00002797.

222 Email from Michael Gula to Brielle Appelbaum, "Fwd: My memory of the call with Chain Bridge Bank," May 9, 2020, BFM000137279 - 280 at 279; Email from Heather Schoeppe to Mike Richardson, "Re: Blue Flame Medical incoming wire 450 million," March 25, 2020, CBB00000686 - 695 at 692.

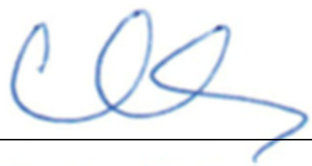
223 Email from Heather Schoeppe to Mike Richardson, "Re: Blue Flame Medical incoming wire 450 million," March 25, 2020, CBB00000686 - 695 at 686 - 687 and 691 - 692; Emails between Mike Richardson and Maria Cole, cc'ing Heather Schoeppe, "Re: Blue Flame Medical incoming wire 450 million," March 25 - 26, 2020, CBB00000686 - 695 at 689 - 691.

224 "How ICS and CDARS Work," ICS & CDARS, available at https://www.icsandcdars.com/how-it-works, accessed February 3, 2021; "IntraFi Network: Certificate of Deposit Account Registry Service, or CDARS," American Bankers Association, available at https://www.aba.com/member-tools/industry-solutions/endorsed-solutions/promontory-interfinancial-network-certificate-deposit-account-registry-service, accessed February 3, 2021.

225 "How ICS and CDARS Work," ICS & CDARS, available at https://www.icsandcdars.com/how-it-works, accessed February 3, 2021.

bank's consideration of opening a CDARS account in response to a large deposit does not suggest that the large deposit imposes any additional regulatory requirements on the bank.

Submitted on February 12, 2021.



Charles H. Grice

Exhibit 1
Example News Releases and Regulatory Guidance Issued by Law Enforcement and Regulatory Entities on Fraudulent Activity During the COVID-19 Pandemic
March 16, 2020 - June 23, 2020

Source	Date	Entity	Description
[1]	March 16, 2020	Financial Crimes Enforcement Network ("FinCEN")	FinCEN advised U.S. financial institutions to "remain alert about malicious or fraudulent transactions similar to those that occur in the wake of natural disasters." FinCEN was also "monitoring public reports and BSA reports of potential illicit behavior connected to COVID-19," including "[i]mposter scams," "[i]nvestment scams," "[p]roduct scams," and "[i]nsider trading."
[2]	March 18, 2020	U.S. Attorney's Office for the Eastern District of Virginia	The U.S. Attorney for the Eastern District of Virginia warned of numerous scams related to COVID-19, including "supply scams" that "claim[] to sell medical supplies currently in high demand, such as surgical masks," and urged the public to take certain steps by being "wary of any business … requesting payments … by wire transfer" and avoiding "send[ing] money through any of these channels."
[3]	March 25, 2020	Federal Financial Institutions Examination Council ("FFIEC")	FFIEC members were "actively discussing and identifying appropriate measures, both collaboratively and individually, to maintain safety and soundness [of U.S. financial institutions] while protecting consumers."
[4]	March 27, 2020	Federal Bureau of Investigation ("FBI")	The FBI warned the health care industry of "increased potential for fraudulent activity dealing with the purchase of COVID-19-related medical equipment" in which "scammers may promise equipment they do not have access to[.]" The FBI asked the medical community to "exercise due diligence and appropriate caution when dealing with any vendors with whom they have never worked and/or of which they've never heard, and when relying on unidentified third-party brokers in the supply chain." The FBI urged individuals to be alert to counterfeit products including N95 respirator masks.
[5]	April 3, 2020	FinCEN	FinCEN updated its March 16, 2020 news release, noting that "[c]ompliance with the Bank Secrecy Act (BSA) remains crucial to protecting our national security by combating money laundering and related crimes, including terrorism and its financing. FinCEN expects financial institutions to continue following a risk-based approach, and to diligently adhere to their BSA obligations." FinCEN also noted that it will "continue outreach to regulatory partners and financial institutions to ensure risk-based compliance with the BSA, and FinCEN will issue additional new information as appropriate."
[6]	April 7, 2020	Office of the Comptroller of the Currency ("OCC")	The OCC supported the risk-based approach to BSA compliance laid out in the April 3, 2020 updated FinCEN COVID-19 notice.

Exhibit 1
Example News Releases and Regulatory Guidance Issued by Law Enforcement and Regulatory Entities on Fraudulent Activity During the COVID-19 Pandemic
March 16, 2020 - June 23, 2020

Source	Date	Entity	Description
[7]	April 13, 2020	FBI	The FBI issued a warning about "rapidly emerging fraud trends related to procurement of personal protective equipment (PPE)" perpetrated specifically against "state government agencies." The FBI noted that these agencies "wire transferred funds to fraudulent brokers and sellers in advance of receiving [PPE] items." The FBI also warned of transactions where a "seller or broker is not an entity with which the buyer has an existing business relationship," a "seller or broker cannot clearly explain the origin of the items or how they are available given current demand," where potential buyers "cannot verify with the product manufacturer that the seller is a legitimate distributor," and where there is "[u]nexplained urgency to transfer funds." On the same day, the FBI warned about bad actors "manipulating the COVID-19 pandemic to their advantage" by "selling fake COVID-19 test kits and unapproved treatments."
[8]	May 18, 2020	FinCEN	In its advisory to financial institutions, FinCEN noted that "[d]etecting, preventing, and reporting" COVID-19-related scams was "critical to our national security." Financial indicators of such scams may include "[a] newly-opened account [that] receives a large wire transaction that the accountholder failed to mention during the account opening process" and a merchant that "cannot explain the source of the goods or how the merchant acquired bulk supplies of highly sought-after goods related to the COVID-19 pandemic." Other red flags include when a seller is "reluctant to provide … the financial institution that is processing the transactions with invoices or other documentation supporting the stated purpose" of the transaction, and when a financial institution "does not understand the merchant's business model" or has "difficulty determining the true nature of the company and its operations."
[9]	June 23, 2020	Federal Reserve Board, Federal Deposit Insurance Corporation, OCC, National Credit Union Administration, State Financial Regulators	The regulatory agencies issued interagency examiner guidance for assessing safety and soundness of U.S. financial institutions during the COVID-19 pandemic. They noted that in response to the COVID-19 pandemic, "[r]apid changes in operational processes and increasing fraud … may result in a heightened operational risk environment."

Exhibit 1
Example News Releases and Regulatory Guidance Issued by Law Enforcement and Regulatory Entities on Fraudulent Activity During the COVID-19 Pandemic
March 16, 2020 - June 23, 2020

Sources:

[1]: "The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity," Financial Crimes Enforcement Network, March 16, 2020, available at https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions, accessed February 5, 2021.

[2]: "U.S. Attorney Warns of Coronavirus Scams Targeting Vulnerable Victims," The United States Attorney's Office for the Eastern District of Virginia, March 18, 2020, available at https://www.justice.gov/usao-edva/pr/us-attorney-warns-coronavirus-scams-targeting-vulnerable-victims, accessed February 5, 2021.

[3]: "Financial Regulators Highlight Coordination and Collaboration of Efforts to Address COVID-19," Federal Financial Institutions Examination Council, March 25, 2020, available at https://www.ffiec.gov/press/pr032520.htm, accessed February 5, 2021.

[4]: "FBI Warns Health Care Professionals of Increased Potential for Fraudulent Sales of COVID-19-Related Medical Equipment," Federal Bureau of Investigation, March 27, 2020, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-health-care-professionals-of-increased-potential-for-fraudulent-sales-of-covid-19-related-medical-equipment, accessed February 5, 2021.

[5]: "The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic," Financial Crimes Enforcement Network, April 3, 2020, available at https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial, accessed February 5, 2021.

[6]: "Bank Secrecy Act/Anti-Money Laundering: OCC Supports FinCEN's Regulatory Relief and Risk-Based Approach for Financial Institution Compliance in Response to COVID-19," Office of the Comptroller of the Currency, April 7, 2020, available at https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-34.html, accessed February 5, 2021.

[7]: "FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic," Federal Bureau of Investigation, April 13, 2020, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic, accessed February 10, 2021. *See also* "FBI Warns of Emerging Health Care Fraud Schemes Related to COVID-19 Pandemic," Federal Bureau of Investigation, April 13, 2020, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-emerging-health-care-fraud-schemes-related-to-covid-19-pandemic, accessed February 5, 2021.

[8]: "Advisory on Medical Scams Related to the Coronavirus Disease 2019," FinCEN Advisory FIN-2020-A002, May 18, 2020, pp. 1 - 2, 4, and 8, available at https://www.fincen.gov/sites/default/files/advisory/2020-05-18/Advisory%20Medical%20Fraud%20Covid%2019%20FINAL%20508.pdf, accessed February 5, 2021.

[9]: "Interagency Examiner Guidance for Assessing Safety and Soundness Considering the Effect of the COVID-19 Pandemic on Financial Institutions," Federal Deposit Insurance Corporation, June 23, 2020, available at https://www.fdic.gov/news/financial-institution-letters/2020/fil20064.html, accessed February 5, 2021; "Interagency Examiner Guidance for Assessing Safety and Soundness Considering the Effect of the COVID-19 Pandemic on Institutions," Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, National Credit Union Administration, and State Financial Regulators, June 2020, pp. 1 and 9, available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20200623a1.pdf, accessed February 5, 2021.