EXHIBIT 8

CONFIDENTIAL

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

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.

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

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.