EXHIBIT 104

[REDACTED]

HIGHLY CONFIDENTIAL UNDER PROTECTIVE ORDER

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 (LMB/IDD)
CHAIN BRIDGE BANK, N.A., Third-Party Plaintiff, v. JPMORGAN CHASE BANK, N.A., Third-Party Defendant.	

EXPERT REPORT OF TERESA A. PESCE

ON BEHALF OF THIRD-PARTY DEFENDANT

JPMORGAN CHASE BANK, N.A.

February 12, 2021

TABLE OF CONTENTS

Page

I. ASSIGNMENT 1

II. QUALIFICATIONS 1

III. SUMMARY OF OPINION 2

IV. FACTUAL AND REGULATORY BACKGROUND 2

A. STATEMENT OF FACTS 3

1. JPMorgan Chase Bank, N.A. and Chain Bridge Bank, N.A. 3

2. The $456 Million Wire Transfer 3

B. REGULATORY AND ENFORCEMENT LANDSCAPE 5

1. Bank Secrecy Act, Patriot Act, and Related Regulations 5

2. Regulatory Expectations 6

3. Enforcement and Penalties 8

4. COVID-19/PPE 8

V. EXPERT OPINION 9

I. ASSIGNMENT

I have been engaged by Wilmer Cutler Pickering Hale and Dorr LLP (WilmerHale), counsel for Third-Party Defendant JPMorgan Chase Bank, N.A. (JPMC). I have been retained based on my expertise, experience, and knowledge of the laws, regulations, regulatory expectations, and enforcement environment in the area of financial crimes, in particular with respect to requirements and expectations driven by the Bank Secrecy Act (BSA), as amended by the USA PATRIOT Act (Patriot Act). I have been asked to apply my expertise, experience, and knowledge to the circumstances of this case; specifically, WilmerHale asked me to provide my opinion on the following question: Whether JPMC acted in line with regulatory requirements and expectations in addressing the March 26, 2020 funds transfer payment it processed on behalf of originator, the California State Treasurer's Office (CSTO), to and through Chain Bridge Bank, N.A. (Chain Bridge), for credit to ultimate beneficiary Blue Flame Medical LLC (Blue Flame).

In furtherance of this assignment, to assist in my understanding of the facts and circumstances surrounding this matter, WilmerHale provided me with materials produced in discovery in this case, which are referenced and cited herein. My work 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 addressed in this report.

II. QUALIFICATIONS

I am an industry leader and subject matter expert in financial-crimes regulatory enforcement and compliance with a demonstrated history of working in and with the financial services industry, including in government, industry, and consulting. I have led large teams and managed significant projects, and I have designed and implemented financial crimes compliance programs and organizational structures.

I currently own and operate an independent consulting firm, established in September 2020. Prior to establishing my consulting firm, I spent 13 years as a Principal in KPMG's Forensic Advisory Services, serving as Global Head of Anti-Money Laundering and Head of the firm's Financial Crimes Solution. I spearheaded engagements for financial institutions in addressing numerous financial crimes and sanctions issues, including assisting clients facing regulatory enforcement actions, both private and public. I have often been called upon to report directly to law enforcement agents and prosecutors, regulatory agencies, and boards of directors.

Before joining KPMG, I was Executive Vice President and AML Director for the North American operations of HSBC North America. I joined the bank to build out the anti-money laundering (AML) compliance function for all business lines and products in response to a regulatory order imposed in 2003 and lifted by the Office of the Controller of the Currency (OCC) during my tenure in 2006.

Prior to joining HSBC, I was an Assistant United States Attorney in the Southern District of New York, serving as Chief of the Major Crimes Unit, and Deputy Chief of the Criminal Division. From 1999 through 2003, I was responsible for supervision and oversight of all money-laundering and tax prosecutions and worked closely with law enforcement and the financial regulatory agencies responsible for oversight of AML enforcement. During my tenure

at the U.S. Attorney's Office, I investigated and prosecuted numerous cases involving and charging money laundering.

I serve as a Lecturer for the Case Western School of Law, Masters of Financial Integrity program, lecturing on a variety of subjects relevant to anti-money laundering enforcement and compliance, as well as criminal law.

I hold a Bachelor of Arts from Columbia University, where I graduated magna cum laude, Phi Beta Kappa, and I hold a Juris Doctor from Columbia Law School, where I served as Managing Editor of the Law Review and received prizes in Constitutional Law and Trial Advocacy.

I am a recognized industry speaker and have published numerous pieces on financial crimes and enforcement. Additional information, including a complete CV and details pertaining to compensation, is appended hereto at Appendix I.

III. SUMMARY OF OPINION

On March 26, 2020, after consultation with Chain Bridge, JPMC agreed to recall a $456 million payment that CSTO had originated for the account of Blue Flame at Chain Bridge. The wire was to purchase personal protective equipment (PPE) in connection with the COVID-19 virus. By conducting due diligence, JPMC learned of numerous red flags concerning the transaction: Blue Flame had limited, if any, internet presence; the bank account was brand new; the account owner was a political lobbyist with no apparent background or history in the medical supply business; the large amount of the wire was out of character for the Blue Flame account holder; and Chain Bridge, Blue Flame's bank, was uncomfortable with the transaction and was holding the payment. This confluence of red flags must be viewed in the context of regulatory requirements and expectations. This transaction took place in a regulatory environment where bank examiners heavily scrutinize banks to determine if they have sufficient controls in place to do their part in the war against financial crime. If controls are deemed deficient, banks face enforcement actions carrying potential fines, expensive remedial requirements, business impediments, and reputational damage. Considering all these facts and circumstances, it is my opinion that JPMC's actions – conducting due diligence and ultimately agreeing to recall the wire – were in line with regulatory requirements and expectations.

IV. FACTUAL AND REGULATORY BACKGROUND

Before rendering an opinion in this matter, I reviewed materials produced in discovery by JPMC and Chain Bridge, including emails, instant messages, and recorded telephone calls. I reviewed the depositions of Chain Bridge Chief Executive Officer John Brough; Chain Bridge President David Evinger; Rakesh Korpal, JPMC's corporate designee; and Timothy Coffey. I performed independent research with respect to Chain Bridge to better understand the size and nature of its business. I reviewed guidance issued by the Financial Criminal Enforcement Network (FinCEN) and the OCC in or around the same time-period as the events in this case, particularly as such guidance pertained to suspicious activity stemming from the exploitation of extraordinary needs resulting from COVID-19. I considered the regulatory and enforcement landscape against which the events in this case occurred, including the relevant law and

regulations, as well as regulatory guidance and expectations for banks such as JPMC. A list of materials I reviewed is listed in Appendix II.

A. STATEMENT OF FACTS

1. JPMorgan Chase Bank, N.A. and Chain Bridge Bank, N.A.

JPMC is a national bank, chartered by the OCC. It is subject to supervision by the Federal Deposit Insurance Company (FDIC), the Federal Reserve System, and the OCC, its primary regulator. Because of the size and significance of a large and complex institution such as JPMC, it is subject to constant examination by regulatory authorities, with examiners from those authorities maintaining offices on bank premises.[1]

Chain Bridge is located in McLean, Virginia, serving customers in Virginia, and catering to the political community.[2] In its 2019 Annual Report, it reported total assets at $829,186,298.[3] With assets under $1 billion, Chain Bridge is considered a small bank from a regulatory perspective. Its primary regulator is the OCC. Banks of this size are generally subject to less examination scrutiny than larger banks.[4]

2. The $456 Million Wire Transfer

On March 26, 2020, JPMC received a request from its client CSTO to process a wire transaction. (JPMC-00000001.) The wire was in the amount of $456,888,600 and was to be sent through Chain Bridge for credit to the account of ultimate beneficiary, Blue Flame. (JPMC-00000467.)

The wire generated an alert in Global Payment Guardian (GPG), a JPMC monitoring system that screens for possible "suspicious commercial monetary activity." (JPMC-00000004; JPMC-00000470.) That alert was serviced by members of JPMC's Payments Control Team, which reviews and investigates potential suspicious transaction activity. (JPMC-00000469-0470; JPMC-00000003-0005; JPMC-00000009.) Specifically, the wire hit on three specific predetermined criteria to sort out transactions for further review: [redacted] (JPMC-00000092-0093.) Upon notice of these alerts being generated, JPMC contacted CSTO to confirm that it had in fact initiated this transaction. (JPMC-00000019.) Upon receiving confirmation from CSTO, JPMC released the wire to Chain Bridge. (JPMC-00000027.)

Rakesh Korpal (Korpal) is JPMC's Global Head of Sanctions Operations, Payments Controls and Funds Controls, in charge of the Payments Control Team. Upon learning the wire

---

[1] OCC Handbook, Large Bank Supervision, https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/large-bank-supervision/index-large-bank-supervision html.
[2] Chain Bridge Bank, N.A. Website, https://www.chainbridgebank.com/commercial/industry-specific/political-committees.
[3] Chain Bridge Bank, N.A. 2019 Annual Report, https://www.chainbridgebank.com/assets/files/8TiiWnc7.
[4] OCC Handbook, Community Bank Supervision, https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/community-bank-supervision/pub-ch-community-bank-supervision.pdf. Community banks are defined as banks with under $10 billion in assets.

had been processed, he requested information about the transaction from Payments Control Team employees, including Timothy Coffey (Coffey), Vice President, Corporate and Investment Banking/Wholesale Payments Fraud Operations. (JPMC-00000047-0048.) Thereafter, Korpal and his team conducted due diligence on the transaction, including on the beneficiary, Blue Flame.

Among other diligence, Korpal sought to determine whether Blue Flame appeared in the Early Warning System (EWS). (JPMC-00000063.) EWS is a subscription service for banks to both report and receive information in order to mitigate fraud. (Korpal Dep. 281:20-282:6.) He was not able to obtain any information from EWS as Chain Bridge is not an EWS participant. (JPMC-00000063.) Through additional diligence, Korpal learned that Blue Flame had limited, if any, internet presence. (Korpal Dep. 69:18-70:3.)

Korpal and Coffey discussed the matter directly with Chain Bridge executives David Evinger, President, and John Brough, Chief Executive Officer. Evinger expressed concerns about the transaction in a call with Coffey, and he told Coffey that Chain Bridge was holding the funds. (JPMC-00000068.) Korpal subsequently spoke with Evinger and Brough, and they reiterated their concerns about the wire. (CBB00002541.) They told Korpal that the Blue Flame account was "brand new," and that, while the person who opened the Blue Flame account was an existing client, a transaction of this size was out of character. (*Id.*) As they informed Korpal, the account was opened by a "lobbyist," and the wire amount was "very unusual." (*Id.*) Then, in a separate call, Evinger asked Korpal whether JPMC would issue a recall of the wire; Korpal responded that he was comfortable as long as Chain Bridge was holding the payment. (CBB00002544.)

Chain Bridge's concerns with respect to this transaction, as expressed to JPMC, were also reflected in internal Chain Bridge actions and discussions. For example:

> Upon receipt of the wire, before any discussions with JPMC personnel, Chain Bridge placed a hold on the funds at Evinger's direction. (CBB00000728.)
>
> In an email exchange between Brough and Chain Bridge SVP/Branch Manager Heather Schoeppe, Brough states that he had spoken to the account owner, but that he and Evinger were skeptical about the wire, and that Peter Fitzgerald, Chairman of Chain Bridge, thought it was a scam. (CBB00000761.)
>
> In a separate exchange between Schoeppe and Mike Richardson, Chain Bridge SVP/Commercial Banking Manager, Schoeppe reported that Evinger and Brough thought that it was strange for a company established two days ago to win such a huge contract from California, and Richardson expressed skepticism about the transaction. (CBB00000667-0668.)

After consultation with Chain Bridge, JPMC agreed with Chain Bridge to recall the funds and then returned the funds to California.

B. REGULATORY AND ENFORCEMENT LANDSCAPE

1. Bank Secrecy Act, Patriot Act, and Related Regulations

Banks are subject to substantial regulation with respect to financial crimes, and in particular BSA/AML compliance. The BSA, as amended by the Patriot Act, and its implementing regulations, provide the foundation for financial institutions' financial crimes compliance program requirements.[5] The BSA is the primary AML law in the United States.[6] But the BSA's intent is not only to detect and prevent money laundering. Rather, the original purpose, as stated, is to require banks to provide information that has "a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism."[7]

The amendment of the BSA through enactment of the Patriot Act substantially increased regulatory requirements. Prior to its enactment, the BSA focused on mandatory reporting. The Patriot Act enhancements were intended in part to require banks to detect and prevent terrorist financing.[8] However, they impose broad coverage impacting all aspects of banking and bank customers in an effort to prevent financial crime. Importantly, the introduction of these new requirements set off a dramatic increase in enforcement activity.

Implementing BSA regulations mandate that financial institutions report on, among other things:

> any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $5,000 or more in funds or other assets where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations or that it was used to facilitate a criminal transaction, and the bank has substantial basis for identifying a possible suspect or group of suspects.[9]

Federal criminal violations are defined broadly; federal offenses such as money laundering and racketeering can be based on an extensive list of underlying criminal offenses, including offenses under state laws.[10]

---

[5] 31 U.S.C § 5311 *et seq*.
[6] The BSA provides programmatic requirements as well as penalties for noncompliance. Money laundering is a separate federal crime. *See* 18 U.S.C §§ 1956, 1957.
[7] 31 U.S.C. § 5311.
[8] *See* FinCEN Website, https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act.
[9] 12 CFR § 21.11(c)(2).
[10] Criminal money laundering laws penalize the laundering of "specified unlawful activity." The list of such activity is extremely broad and can be found at 18 U.S.C. § 1956(c)(7).

The recently implemented Customer Due Diligence, or CDD, Rule, further requires financial institutions to monitor for unusual activity. Under the Rule, a bank is responsible for, among other things:

- understanding the nature and purpose of the customer relationships; and
- conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[11]

This reinforces a bank's obligation to assess its customer's transactions and better understand whether activity is in line with what is expected for the account. Understanding a transaction requires understanding all parties.

2. Regulatory Expectations

The written statutory and regulatory requirements set the floor for a BSA/AML compliance program. Regulatory expectations far exceed the letter of the law. Banks are expected to have proactive, risk-based programs that are commensurate with the size and risk profile of the institution. Failure to maintain or effectively execute a program can result in significant penalties, regardless of whether requirements are codified.

The Federal Financial Institution Examination Council, which is comprised of members of the OCC, the Federal Reserve, the FDIC, the National Credit Union Administration (NCUA), the Consumer Financial Protection Bureau (CFPB), and the State Liaison Committee, issues a BSA/AML Exam Manual (the FFIEC Manual),[12] providing examiners detailed guidelines on how to conduct a BSA/AML exam applying a risk-based approach with laws and regulations as a baseline.[13] The FFIEC Manual, in particular, directs examiners to focus on products and services presenting elevated risk and calling for enhanced controls. Upon release of the FFIEC Manual, the OCC directed banks under its supervision to "familiarize themselves" with it and update their BSA/AML compliance programs accordingly.[14] Similarly, FinCEN, an agency of the U.S. Treasury Department responsible for enacting regulation to implement the BSA and Patriot Act, frequently issues guidance to banks interpreting the meaning and spirit of regulations, further instructing banks on what is expected for program compliance.[15]

Large banks are subject to enhanced scrutiny. As noted, a team of examiners dedicated to that bank only will reside on the bank's premises.[16] Exams can be more focused – e.g. covering particular lines of business or single program elements – and they can be ongoing.

---

[11] FinCEN Guidance, FIN-2016-G003 (July 19, 2016).
[12] The last complete FFIEC Manual was issued in 2014. It was supplemented in April 2020.
[13] For example, the FFIEC Manual directs examiners to review and assess a bank's risk assessment both to determine whether it accurately describes the bank's risk profile and control environment, and to use as a baseline in conducting the examination. There is, however, no law or regulation mandating that banks conduct a risk assessment. Rather, this is a regulatory expectation, and it is often a subject in enforcement actions. *See e.g.*, *In the Matter of M.Y. Safra Bank, FSB*, OCC Consent Order 2020-005, at Article X (Jan. 30, 2020) (requiring Safra to "develop a written institution-wide, ongoing" BSA/AML risk assessment).
[14] OCC Bulletin 2014-60 (December 2, 2014).
[15] *See* FinCEN Website, https://www.fincen.gov/resources/statutes-regulations/guidance.
[16] *See* fn 1.

Lines of business or products considered higher risk are often the subject of a discrete exam. Exams and examiners require substantial and sustained attention from bankers and compliance officers, irrespective of business disruption. Bank examiners can access customer, transactional, and other bank information when conducting BSA/AML exams, in the interest of financial crime prevention.

Banks are expected to understand their risk profile and to manage their risks with mitigating controls. Higher risks (e.g. high-risk customers, high-risk products, high-risk transactions) must be mitigated with more stringent controls, commensurate with that risk. Critical components of a BSA/AML program are those requiring banks to understand and conduct due diligence on their customers and understand their expected activity, and to determine whether activity flowing to or through the bank may be suspicious.[17]

To assist in discharging their regulatory requirements and expectations, banks rely on automated detection systems for monitoring transactions. These systems identify anomalies in transactional activity and provide a run of alerts for analysts to review after the transactions have occurred and been processed. Some automated systems focus on allowing a bank to detect and, if necessary, report suspicious activity, but not necessarily prevent potentially unlawful transactions. Other systems generate alerts as activity is conducted; such systems focus on preventing loss to customers or the bank and allow for a more immediate response. These systems share a common goal in identifying suspicious activity for further review, and financial institutions use the output from these systems for multiple related purposes, including detection of potential fraud, potential money laundering, or other financial crimes.

Given the obligation to report any "known or suspected Federal criminal violation," the nature of the activity that must be detected and reported far exceeds money laundering; banks are required to detect and report potentially unlawful or unusual activity they have identified.[18] In the case of egregious suspicious activity, banks are advised to notify law enforcement directly,[19] and they can be criticized or even penalized for not terminating relationships with very high-risk customers or with customers whose accounts are used to process suspicious transactions.[20] Banks are not obligated to do business with parties they believe present enhanced risk; they often implement internal watchlists consisting of names of individuals or entities for further scrutiny, or with whom they do not wish to do business. If a party to a transaction hits a watchlist filter,

---

[17] International guidance specifically calls upon beneficiary banks to have procedures in place to reject or suspend payments lacking sufficient information when appropriate. The Financial Action Task Force or FATF's International Standards on Combatting Money Laundering and the Financing of Terrorism – the FATF Recommendations – provides a foundation for global financial crimes regimes. Recommendation 16, Interpretive Note 16, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/fatf%20recommendations%202012.pdf; *see also* The Wolfsburg Group, Payment Transparency Standards, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/1.%20Wolfsberg-Payment-Transparency-Standards-October-2017.pdf.

[18] The SAR form contains eleven categories of activity, each with multiple sub-categories of more detailed unlawful behaviors. In addition to the enumerated acts, each category has a box for "other." *See* FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Requirements User Guide at 88-93 (July 2020).

[19] 31 C.F.R. § 1020.320(b)(3).

[20] *See, e.g.*, U.S. Bancorp – Deferred Prosecution Agreement (S.D.N.Y Feb. 12, 2018).

the transaction may alert even if no other rules breach. (*See, e.g.*, JPMC-00000356; Korpal Dep. 180:1-7.)

3. Enforcement and Penalties

When examiners find lapses or gaps in a bank's financial crimes compliance program, the bank can be subject to enforcement activity. This could range from findings in Reports of Examination (ROEs), such as Matters Requiring Attention (MRAs), which require banks to devise a plan to remediate identified issues; it could lead to a non-public enforcement action, where program element failures are called out and the bank is given a window of opportunity to address the open issues; or it could result in public enforcement actions, potential criminal charges, and fines. Charges can be levied against individuals in addition to the institutions they represent. Enforcement activity is costly to a bank; irrespective of whether fines are imposed, remediation can be very expensive, and reputational risk can impair business. Moreover, BSA/AML enforcement actions can put banks in the so-called "penalty box"; regulators can bar financial institutions from engaging in certain business transactions until the regulators, at their discretion, lift the bar.

Banking regulators, including the OCC, have actively enforced BSA/AML requirements, imposing a substantial number of public enforcement actions against banks since the enactment of the Patriot Act. The provisions of these enforcement actions and the mandates imposed on banks pursuant to such enforcement actions exceed those imposed by law and regulation.[21] In cases where a bank is perceived to have a systemic or programmatic failure, criminal charges can accompany civil penalties, and a monitor may be appointed to ensure the bank meets its remedial obligations.[22]

4. COVID-19/PPE

Recently, regulatory focus has shifted to the COVID-19 crisis. In early 2020, FinCEN began issuing numerous warnings to banks to be alert to illicit activity related to the COVID-19 pandemic. The alerts detail a number of different frauds and scams that have become prevalent since the onset of COVID-19, and FinCEN expressly directed banks to keep up to date with continuing guidance in order to fulfill their obligations under the BSA.[23] In particular, on March 16, 2020, FinCEN issued guidance specifically on "Product Scams," warning banks to be alert to frauds involving the fraudulent marketing of COVID-19 related supplies, "such as certain

---

[21] *See, e.g.*, *In the Matter of Capital One, National Association, McLean, Virginia*, FinCEN Assessment of Civil Money Penalty No. 2021-01 (Jan. 15, 2021); *In the Matter of M.Y. Safra Bank, FSB*, OCC Consent Order 2020-005 (Jan. 30, 2020); *see also In the Matter of U.S. Bank National Association,* OCC Consent Order 2015-113 (October 23, 2015) (requiring, *inter alia*, a risk assessment, and an electronic due diligence database); *In the Matter of Citibank, N.A.*, OCC Consent Order 2012-052 (April 5, 2012) (requiring risk assessment, electronic database, specific account closure procedures).

[22] The Department of Justice entered into Deferred Prosecution Agreements mandating monitorships for criminal violations of the BSA. *See, e.g.*, *HSBC Bank U.S.A., N.A. et al.* – Deferred Prosecution Agreement (E.D.N.Y. Dec. 12, 2012). These actions can name individuals as well as institutions. Moreover, individuals and institutions can be charged with the actual crime of Money Laundering if they turn a blind eye to suspicious activity they know is occurring. *See U.S. v. Flores*, 454 F.3d 149 (3d Cir. 2006).

[23] FinCEN Website, https://www.fincen.gov/coronavirus.

facemasks."[24] This guidance cautioned banks to monitor for and report COVID-19-related suspicious transactions, directing them to explicitly reference "COVID19" in their reporting templates.

V. EXPERT OPINION

Based on the facts and circumstances set forth above, and based upon my subject matter expertise, knowledge, and experience in the field of financial crimes compliance and enforcement, it is my opinion that JPMC acted in line with regulatory requirements and expectations when it questioned, investigated, and, after consultation with Chain Bridge, agreed to recall the March 26, 2020 wire.

As explained, banks – and especially large financial institutions like JPMC – face strict regulatory scrutiny. They are required to apply risk-based policies, procedures, and controls to prevent, detect, and report suspicious activity. Failure to exercise strict controls, including conducting sufficient due diligence on customers and transactions, puts them at regulatory risk. Resident examiners will closely scrutinize a bank's ability to mitigate financial-crimes risk commensurate with the inherent risks in each of their businesses and business activities, and they will prioritize a bank's ability to exercise financial crimes controls over a bank's business interests.

The Blue Flame transaction raised numerous flags – including the exceptionally large amount – warranting JPMC's due diligence. JPMC released the wire to Chain Bridge only after contacting its client, CSTO, and CSTO confirmed that it had in fact initiated this transaction and intended for it to be processed. But, consistent with regulatory expectations, given the red flags with the transaction, JPMC prudently did not stop with CSTO's confirmation and the release of the wire to Chain Bridge. Rather, the Payments Control Team conducted further due diligence into potential suspicious elements of the transaction.

The GPG system flagged the transaction as possible suspicious commercial monetary activity, alerting against three objective rules: [redacted] (JPMC-00000092.) The GPG alert additionally revealed that the transaction was more than four times the size of the average transaction for this customer (*i.e.*, CSTO) across the last 18 months. (JPMC-00000003.) These are common typologies in automated monitoring systems, and consistent with regulatory guidance.[25] Each of the three alerts was a red flag – a basis for suspicion – warranting further investigation.

---

[24] FinCEN Website, https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions.

[25] Transaction monitoring systems provide scenarios that can be tailored to suit an institution's risk tolerance. They can be based on commonly reported red flags or can be more customized. Most banks will set a dollar threshold, above which a transaction is reviewed. Volume and velocity of payments are also common scenarios. For a discussion on transaction monitoring, *see* FFIEC at 64-66 (discussing, inter alia, how vendor systems generally use discretionary dollar thresholds for alert generation and how reports will focus on identifying larger funds transfer transactions). *See also, e.g.*, FFIEC at F-1, F-2, F-3 (red flags including the following: "Funds transfer activity is unexplained…"; "The customer's background differs from that which would be expected on the basis of his or her

The Payments Control Team in turn performed the duties expected of financial crimes professionals by conducting due diligence on the transaction. Funds transfers are considered higher risk activity by examiners.[26] Such transfers present enhanced risk as money is passing to a third-party beneficiary who is not the bank's customer and is therefore unknown to the bank. When funds transfers alert, banks must conduct sufficient due diligence, among other things, to understand all parties to the transaction – their customer, in this case the originator of the transaction, and the unknown third party, the beneficiary. Here, two of the reasons the transaction alerted pertained to the beneficiary – with which JPMC had no relationship. Accordingly, consistent with regulatory expectations, the Payments Control Team sought to obtain information about that unknown party.

Based on my experience and expertise, investigators assessing transactions will seek to understand, among other things, who the beneficiary is, what type of business they conduct, what history and reputation the party has in that business, and whether there is any other negative media/information to be gleaned from public data sources. The purpose of this investigation is to determine whether the transaction appears normal and expected for these parties. Moreover, the CDD Rule requires banks to understand their customer's transactional activity. But transactions can only be understood when all the parties to the transaction are fully identified, and the reason for the transaction is transparent.

The Payments Control Team's diligence uncovered additional red flags. To better understand the beneficiary, Korpal spoke to Chain Bridge's President, David Evinger, and Korpal learned that Evinger himself was uncomfortable with the transaction. Per Evinger, the Blue Flame account was "brand new." Thus, Blue Flame would have no historical activity against which Chain Bridge or JPMC could judge the CSTO transaction. There could be no indication that this transaction was normal and expected for Chain Bridge's customer, Blue Flame. Moreover, while one of Blue Flame's owners had other accounts with Chain Bridge, Evinger was clear that a transaction of this enormity was out of character for his client.

Critically, based on its own suspicion, Chain Bridge was holding the funds and had not released them to Blue Flame's account. (CBB00002544.) This would have provided JPMC and Korpal a reasonable degree of comfort irrespective of Chain Bridge's request that JPMC recall the wire. The potentially suspicious activity, while perhaps attempted, was prevented, allowing Korpal to continue his due diligence knowing that the transaction would not be completed.

Korpal also requested that his colleagues conduct searches on Blue Flame. Such searches are routinely run when conducting due diligence on customers or parties to a transaction. These searches, again, produced additional red flags: Blue Flame Medical LLC had limited, if any, internet presence (Korpal Dep. 69:18-70:3), which would further appropriately create doubt as to the legitimacy of the transaction. And, as Chain Bridge informed Korpal, the Blue Flame account owner was a lobbyist, with no apparent history in the medical supply business.

These red flags must be viewed against the COVID-19 backdrop. In addition to news reports of fraud, FinCEN specifically issued alerts to the banking industry to be watchful for

---

business activities"; "Customer makes high-value transactions not commensurate with the customer's known incomes"; "Payments or receipts with no apparent link to legitimate contracts, goods or services are received").

[26] *See* FFIEC 19-20.

"illicit behavior" connected to COVID-19. They warned banks to use extreme caution when processing transactions. In particular, on March 16, 2020, FinCEN issued guidance that explicitly called out the potential for fraud in the purchase of medical supplies.[27] FinCEN and the OCC have continued to issue COVID-related fraud alerts. Importantly, FinCEN has directed banks to stay up to date with continuing guidance on COVID-related frauds to ensure compliance with the BSA's requirements.[28] Indeed, Coffey testified that JPMC had investigated a number of COVID-related cases and had a heightened awareness of COVID-related fraud. (Coffey (Rough) Dep. 102.)

Given the opportunity to prevent a potentially illegitimate $456 million transaction, JPMC's Payments Control Team acted reasonably and in line with regulatory expectations by consulting with Chain Bridge and thereafter agreeing with Chain Bridge to recall the payment. JPMC performed due diligence that examiners would demand given the size of the transaction and the many red flags. Knowing that the payment was being held by Chain Bridge, JPMC acted reasonably in assisting the prevention of what could have been a substantial loss to its client. Knowingly letting such a large sum go to an entity with limited, if any, internet presence, with no medical supply history, that had established accounts only the day before, that was controlled by a political lobbyist with no medical supply history, and whose own bank was uncomfortable with the transaction would have been out-of-line with regulatory expectations.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: February 12, 2021

TERESA A. PESCE

[27] *See* fn 24.
[28] *See* fn 23-24.