UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:	)	
	)	**Number 2021-03**
CommunityBank of Texas, N.A.	)	
	)	

CONSENT ORDER IMPOSING CIVIL MONEY PENALTY

The Financial Crimes Enforcement Network (FinCEN) conducted a civil enforcement investigation and determined that grounds exist to impose a Civil Money Penalty against CommunityBank of Texas, N.A. (CBOT or the Bank) for violations of the Bank Secrecy Act (BSA) and its implementing regulations.[1] CBOT admits to the Statement of Facts and Violations set forth below and consents to the issuance of this Consent Order.

I. JURISDICTION

Overall authority for enforcement and compliance with the BSA lies with the Director of FinCEN, and the Director may impose civil penalties for violations of the BSA and its implementing regulations.[2]

At all times relevant to this Consent Order, CBOT was a "bank" and a "domestic financial institution" as defined by the BSA and its implementing regulations.[3] As such, CBOT was required to comply with applicable FinCEN regulations.

---

1 The BSA is codified at 31 U.S.C. §§ 5311-5314, 5316-5336 and 12 U.S.C. §§ 1829b, 1951-1959. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.

2 31 U.S.C. § 5321(a); 31 C.F.R. §§ 1010.810(a), (d); Treasury Order 180-01 (July 1, 2014).

3 31 U.S.C. § 5312(b)(1) (defining domestic financial institution); 31 C.F.R. § 1010.100(d) (defining bank).

II. STATEMENT OF FACTS

The conduct described below took place beginning on or about January 1, 2015, and continuing until on or about December 31, 2019 (the Relevant Time Period), unless otherwise indicated.

Background

Bank Secrecy Act

The BSA requires banks to implement and maintain an effective anti-money laundering (AML) program in order to guard against money laundering through financial institutions.[4] Additionally, the BSA imposes affirmative duties on banks such as CBOT, including the duty to identify and report suspicious transactions relevant to a possible violation of law or regulation in suspicious activity reports (SARs) filed with FinCEN.[5] The reporting and transparency that financial institutions provide through these reports is essential financial intelligence that FinCEN, law enforcement, and others use to safeguard the U.S. financial system and combat serious threats, including money laundering, terrorist financing, organized crime, corruption, drug trafficking, and massive fraud schemes targeting the U.S. government, businesses, and individuals.[6]

FinCEN

FinCEN is a bureau within the U.S. Department of the Treasury and is the federal authority that enforces the BSA by investigating and imposing civil money penalties on financial institutions and individuals for willful and negligent violations of the BSA.[7] As

4 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210.

5 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320.

6 FinCEN, *FIN-2014-A007, FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance* (Aug. 11, 2014).

7 31 U.S.C. § 5321(a). In civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose. The Bank admits to "willfulness" only as the term is used in civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1).

delegated by the Secretary of the Treasury, FinCEN has "authority for the imposition of civil penalties" and "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter," including the Office of the Comptroller of the Currency (OCC).[8]

The OCC

The OCC is a federal banking agency within the U.S. Department of the Treasury that has both delegated authority from FinCEN for examinations and separate authority under Title 12 of the United States Code for compliance and enforcement. Under this authority, the OCC conducts regular examinations and issues reports assessing a bank's AML and BSA compliance.[9]

CommunityBank of Texas, N.A.

The Bank is a wholly owned subsidiary of CBTX, Inc., a bank holding company incorporated in 2007, that operates 35 branches in Texas—19 in the Houston market area, 15 in the Beaumont/East Texas market, and one in Dallas.[10] The Bank provides various banking products and financial services to small and mid-sized businesses and professionals operating within the Bank's markets. During the Relevant Time Period, the Bank was a "financial institution" and a "bank" within the meaning of the BSA and its implementing regulations[11] and was subject to an annual examination performed by the OCC as its Federal functional regulator.

8 31 C.F.R. § 1010.810(a), (d).

9 12 U.S.C. § 1818(s)(2); 12 C.F.R. § 21.21.

10 SEC 10-Q as of June 30, 2021, *available at* https://www.sec.gov/ix?doc=/Archives/edgar/data/1473844/000155837021009469/cbtx-20210630x10q.htm.

11 31 U.S.C. § 5312(a)(2)(A); 31 C.F.R. §§ 1010.100(d)(1), 1010.100(t)(1).

The Bank Failed to Implement an Adequate Anti-Money Laundering Program

In order to guard against money laundering, the BSA and its implementing regulations require banks with a Federal functional regulator, such as the OCC, to establish an AML program that is reasonably designed and includes at a minimum: (a) provides for a system of internal controls to ensure ongoing compliance; (b) provides for independent testing for compliance conducted by bank personnel or by an outside party; (c) designates an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (d) provides training for appropriate personnel.[12] The Bank willfully failed to implement an AML program that adequately met these BSA requirements during the Relevant Time Period.

Establishment of AML Program

During the Relevant Time Period, the Bank had an AML program in place. However, as implemented, the Bank's AML program was not adequate to meet the minimum requirements of the BSA and guard against money laundering. As designed, the Bank utilized an enterprisewide automated AML monitoring system that reviewed transactions and generated alerts of possible suspicious activity ("case alerts") based on predetermined criteria; thereafter, case alerts were to be sent to an AML analyst to review the activity. Activity that was deemed suspicious was to be raised to a SAR committee, and, where appropriate, a SAR would be filed. In practice, however, the Bank's AML program failed to operate as designed.

Inadequate Resources

CBOT's AML compliance office was understaffed. During the Relevant Time Period, the Bank retained six to eight BSA staff, including a BSA Officer and several BSA analysts, of which three reviewed case alerts on a regular basis and provided quality-control review for one another. Those three BSA analysts each reviewed an average of

12 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210 (2015); 31 C.F.R. § 1020.210(c) (2018); 12 C.F.R. §§ 21.21(c)(1), 21.21(d).

100 case alerts per day, which meant that BSA analysts often did not review supporting documents (cash deposit slips, wire transcripts, check images, etc.), although all of this information was readily available. This understaffing and failure to allocate sufficient resources further exacerbated the other failures identified below.

Customer Due Diligence (CDD)

FinCEN regulations require an AML program to include "[a]ppropriate risk-based procedures for conducting ongoing" CDD.[13] FinCEN has issued guidance to financial institutions regarding their CDD requirements. This guidance states that financial institutions such as banks "must establish policies, procedures, and processes for determining whether and when, on the basis of risk, to update customer information to ensure that customer information is current and accurate."[14] A bank "should have an understanding of the money laundering, terrorist financing, and other financial crime risks of its customers" in order to develop a "customer risk profile."[15] The guidance also states, "[s]hould the financial institution become aware as a result of its ongoing monitoring of a change in customer information . . . that is relevant to assessing the risk posed by the customer, the financial institution must update the customer information accordingly. Additionally, if this customer information is relevant to assessing the risk of a customer relationship, then the financial institution should reassess the customer risk profile . . . ."[16]

During the Relevant Time Period, the Bank performed CDD, in part, through its automated AML monitoring system. Under that system, the Bank assigned its customers a risk rating score based on a variety of risk factors, which it obtained through questionnaires for businesses and individuals. By at least 2015, the

13 31 C.F.R. § 1020.210.

14 FinCEN, FinCEN Guidance, FIN-2020-G002, CDD FAQ (Aug. 3, 2020) *available at* https://www.fincen.gov/sites/default/files/2020-08/FinCEN_Guidance_CDD_508_FINAL.pdf.

15 Id.

16 Id.

Bank's policies and procedures required that the front-line staff complete all CDD documentation at account opening after a discussion with the customer, as well as for changes in signature authority over an existing account. Despite these policies, CDD questionnaires were often not updated when circumstances warranted and therefore at times lacked critical information. Where CDD questionnaires were flagged as incomplete, AML staff were instructed to obtain additional information from customer account officers rather than from the customers themselves.

For example, for one customer—a business that operated in several domestic and international High Intensity Drug Trafficking Areas—the Bank failed to ask whether the organization conducted international transactions at account opening, as that question was not part of the Bank's standard CDD questionnaire. The Bank then added the international transactions question to the CDD questionnaire on May 28, 2019, after front line staff had already on-boarded the customer. Thereafter the Bank did not go back to ask that question to the previously on-boarded customer.

Additionally, to establish an understanding of account activity, the Bank reviewed its customers at account opening and again after 90 days to determine whether the customer's activity conformed with the answers provided at account initiation. After the initial review, however, the Bank used an automated system to both monitor customer activity on a daily basis and conduct monthly AML reports that calculated the difference between the expected activity volume provided by the customer and the actual transactional activity. While these reviews compared both a customer's activity to other peers in similar peer-groups, and current customer account activity to prior customer account activity, this practice at times failed to enable the Bank to fully understand the nature and legitimacy of its customers' activity and patterns based on their business models. For example, where a customer's transactional activity was consistent with its own prior activity, the automated system was unable to detect whether the original account activity itself was illicit.

The Bank's automated AML monitoring system had the functionality to generate monthly worklist items, such as "High Risk Reports" that could provide information about account activity for high-risk customers. Despite this ability, AML staff did not generate such reports during the ordinary course of business.

Activity Monitoring and Cleared Case Alerts

The Bank's automated AML monitoring system generated a substantial number of case alerts on potentially suspicious activity. To reduce the number of case alerts AML staff had to review, the BSA Officer applied exemptions for customers whose activity was thought to be "well-known," including those individuals later arrested for or convicted of financial crimes, which resulted in lowering the case alerts generated for those customers. For example, in 2019, the Bank's adjustments eliminated approximately 1,000 case alerts that would have been generated and reviewed for customers whose activity was thought to be well-known and who the system alerted on frequently. The Bank did not have work papers or other appropriate documentation supporting the adjustments.

Additionally, the Bank's automated AML monitoring system included a list of possible reasons a case alert could be closed without elevating the matter further. While a pre-set list of possible reasons is not per se improper, Bank analysts often cited those reasons to close case alerts without further analyzing the activity that triggered the alert—even when the BSA analysts knew the customer was already engaging in suspicious activity—and did not provide sufficient support to justify the closure. For example, after filing a SAR on a customer, each time the automated AML monitoring system generated an additional case alert on *new* activity—almost every month—BSA analysts cleared the activity by using the same pre-set reason code, namely: "A SAR was previously filed and is not due for review at this time."

Even where AML analysts did elevate transactions, a number of those alerts ended up closed without further due diligence after discussions with front-line staff, account representatives, or the BSA Officer regarding customer activity. At times, the Bank reported the transaction in a SAR, but even then did not investigate further into the customer or the activity that triggered the case alert.

Unfiled SARs

In addition to the above AML program failures, the AML failures resulted in the below willful failures to timely and accurately file at least 17 SARs.

The Bank Failed to File Suspicious Activity Reports

Background

The BSA and its implementing regulations require banks to report transactions that involve or aggregate to at least $5,000, are conducted by, at, or through the bank, and that the bank "knows, suspects, or has reason to suspect" are suspicious.[17] A transaction is "suspicious" if a bank "knows, suspects, or has reason to suspect" the transaction: (a) involves funds derived from illegal activities, or is conducted to disguise funds derived from illegal activities; (b) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations implementing it; or (c) has no business or apparent lawful purpose or is not the sort in which the customer normally would be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction.[18] A bank is generally required to file a SAR no later than 30 calendar days after the initial detection by the bank of the facts that may constitute a basis for filing a SAR.[19]

17 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320.

18 31 C.F.R. § 1020.320(a)(2)(i)-(iii).

19 31 C.F.R. § 1020.320(b)(3).

To obtain the necessary transparency into potentially illicit activity, FinCEN, law enforcement, and other regulators rely on financial institutions' accurate and timely filing of SARs. To accurately and completely report a SAR, parties involved in the suspicious activity should be identified as a subject of the SAR.[20] Investigators use these names and other identifiers to retrieve relevant records related to the subjects and targets of an investigation. Failure to file a SAR can hamper a law enforcement investigator's or regulator's ability to identify relevant records. Additionally, filing SARs without properly identifying the subjects (*i.e.*, failing to identify all subjects connected to the conduct) can obfuscate the true nature of the activity and those involved.

As described above, while the Bank had an AML program during the Relevant Time Period, the program was not adequately implemented or resourced. As a result, AML analysts did not devote adequate time and attention to case alerts generated by the Bank's automated AML monitoring system. The Bank's BSA Officer undertook, without sufficient justification of AML risk considerations, steps to reduce the number of case alerts reviewed by the Bank's AML analysts. As a consequence, the Bank willfully failed to file at least 17 SARs on suspicious transactions processed by, at, or through the Bank, even when it had reason to believe certain customers were subjects of criminal investigations. The following is a list of examples of the Bank's willful failures to file SARs.

Customer A

Customer A was a customer of the Bank beginning as early as 2007. Customer A owned and operated Business 1—a used car dealership—and Business 2—a financing company. Customer A, through their spouse, Business 1, Business 2, and others held approximately 19 accounts at the Bank. Customer A, Customer A's spouse, and Customer A's businesses were wellknown to the Bank.

20 FinCEN, FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions, Version 1.2 (Oct. 2012) *available at* https://www.fincen.gov/sites/default/files/shared/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf.

Business 1 was a business that purported to sell pre-owned personal vehicles with an average vehicle price of approximately $15,000. Customer A purchased the vehicles from several used car auctions and paid for inventory with checks. Purchased vehicles were then put on the market and car purchase payments were deposited in the account for Business 1 at the Bank. At the same time as Business 1's apparently legitimate used car business cycle was ongoing, Customer A received suspicious deposits to Customer A's Business 1 and Business 2 accounts at the Bank. For example, payments included wire transfers of large round dollar amounts sent by persons known to be gamblers, or included deposits from large-dollar sequentially numbered checks from the same payor that were all deposited on the same day. Customer A often transferred funds between separate business and personal accounts at the Bank, or to Customer A-controlled accounts at other banks, or cashed out large deposits. This activity both lacked an apparent legitimate business purpose, and was indicative of money laundering.

The Bank rated Customer A as a "high-risk" customer and its automated AML monitoring system alerted regularly on activity in accounts controlled by Customer A. The Bank's BSA Officer flagged some of the above activity as suspicious. However, in most cases, CBOT elected not to raise case alerts for possible review, and as a result, the Bank did not file SARs in all appropriate instances. When the BSA Officer raised concerns about possible suspicious activity through Customer A's accounts with the relationship manager and the executive VP Credit Officer, the BSA Officer accepted an implausible explanation about the transfers of funds between Business 1 and Business 2 and ultimately decided not to file a SAR. When the Bank did file SARs on Customer A's accounts, it typically filed them only on structuring activity and—with one exception—not on the other underlying potential money laundering or other suspicious activity.

In June 2019, Customer A, Customer A's spouse, and another family member pleaded guilty to criminal charges including structuring, tax evasion, and money laundering associated with operating an illegal sports gambling operation from at least 1985 until April 2017, including activity that went through Customer A's accounts at the Bank. Despite hundreds of suspicious transactions running through Customer A's accounts over a course of years, repeated alerts on Customer A's accounts from CBOT's automated AML monitoring system, a criminal conviction, and other red flags, CBOT only filed one SAR regarding Customer A's money laundering conduct during the Relevant Time Period.

Customer B

Customer B was a former CPA who in 2013 pled guilty to a tax crime and who contemporaneous public news stories connected to a multibillion dollar sports gambling ring. Despite Customer B's history, the Bank on-boarded Customer B as a customer in 2017 and permitted Customer B to open an account for a social club, which was a gambling establishment. Around the same time the Bank allowed another individual who was affiliated with Customer B to open several other accounts for medical or healthcare businesses, even though neither that individual nor Customer B had any apparent background in managing medical businesses. The Bank failed to timely and adequately complete CDD for Customer B's gambling business, including leaving a question unanswered about whether the business was engaged in gambling.

Customer B's accounts and account activity had various red flags for money laundering or illicit conduct including, but not limited to, using the same business address to register multiple businesses, business accounts that had unexplained periods of dormancy, nominees acting to conceal the actual beneficial owner of accounts, and the absence of ordinary business activities. Further, account analysis shows that Customer B transferred substantial sums between the gambling business and the medical and healthcare businesses.

Despite these various red flags, the Bank failed to timely and accurately file SARs on most of this activity. Where the Bank did file SARs, it failed to name Customer B as a subject, and failed to further investigate the underlying activity that might have led to the identification of additional suspicious activity. Specifically, in 2018 and 2019, the Bank filed three SARs on three large cash deposits into a medical business account based on large cash deposits made into the account. Two of these SARs only named Customer B's associate and the medical business as subjects of the SAR, despite substantial account connectivity between Customer B's accounts and the medical business account. Ultimately, in April 2019, the Bank did file a SAR that named Customer B as a subject, but this SAR inaccurately claimed that the Bank was unaware of Customer B's affiliation with the medical business.

One month later, in May of 2019, Customer B was arrested for allegedly operating an illegal gambling ring out of Customer B's gambling business in Houston. Thereafter, the Bank filed an amended SAR reporting over $30 million in suspicious activity through Customer B's accounts.

Customer C

The Bank on-boarded Customer C and Customer C's family in 2009, and during the Relevant Time Period permitted them to open at least seven business and personal accounts at the Bank, including accounts for Business 3 and Business 4. During on-boarding, the Bank failed to collect complete CDD information for Business 3, including complete information about the nature of the business and accurate information about the legal form of the business.

Customer C and Customer C's family's accounts collectively exhibited multiple red flag indicators of illicit activity such as mass registration addresses, an absence of typical business activities, frequent deposits of checks, and a high volume of fees imposed for insufficient funds. Further, by at least 2018, the Bank was aware of law

enforcement interest in Customer C and Customer C's family, and as a result, in March 2018, the Bank elevated Customer C, Customer C's family, and Customer C's business accounts to the status of high-risk customers. However, in so doing the Bank failed to complete an enhanced due diligence questionnaire reflecting anything unusual about the accounts, including the reason for the risk elevation.

Despite the red flag indicators, the law enforcement interest, and the recognition of Customer C and Customer C's family's high-risk status, the Bank failed to file any SARs on the activity running through their accounts until January of 2020. Even then, these SARs were inadequate to describe the scope of the suspicious activity. In July of 2020, Customer C and several members of Customer C's family were arrested for running a Chemical Trafficking Organization through Business 3 and Business 4. The indictment alleged money laundering through Customer C's accounts at CBOT. In September of 2020, only after the indictment was unsealed, did the Bank file a more substantial SAR that reported the suspicious activity running through Customer C's accounts.

III. VIOLATIONS

FinCEN has determined that CBOT willfully violated the BSA and its implementing regulations during the Relevant Time Period. Specifically, FinCEN has determined that CBOT willfully failed to implement and maintain an effective AML program that was reasonably designed to guard against money laundering, in violation of 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 1020.210. Additionally, FinCEN has determined that CBOT willfully failed to accurately and timely report suspicious transactions to FinCEN, in violation of 31 U.S.C. § 5318(g) and 31 C.F.R. § 1020.320.

IV. ENFORCEMENT FACTORS

FinCEN considered all of the factors outlined in the Statement on Enforcement of the BSA, issued August 18, 2020, when deciding whether to impose a civil money

penalty in this matter.[21] The following factors were particularly relevant to FinCEN's evaluation of the appropriate disposition of this matter, including the decision to impose a civil money penalty and the size of the penalty.

- Nature and seriousness of the violations, including extent of possible harm to the public and systemic nature of the violations. CBOT's violations of the BSA and its implementing regulations were serious and caused significant possible harm to the public. Information that FinCEN reviewed shows that during the Relevant Time Period, CBOT willfully failed to implement and maintain an effective AML program and, as a result, failed to detect and report suspicious or illicit activity conducted by several long-term customers. The Bank failed to implement and maintain an effective AML program despite the presence of numerous and repeated AMLrelated warning signs related to specific highrisk customers. Consequently, CBOT failed to report hundreds of suspicious transactions through the Bank that involved actual illegal activity. On the other hand, CBOT received satisfactory or strong BSA/AML examination findings from outside examiners through 2019.

- Impact or harm of the violations on FinCEN's mission to safeguard the financial system from illicit use, combat money laundering, and promote national security. CBOT's failures permitted money launderers and other criminals to perpetuate their crimes through the U.S. financial system. Law enforcement charged at least three groups of Bank customers with crimes based in part on transactions through their accounts at CBOT. Accordingly, CBOT did real harm to the law enforcement interests reflected in FinCEN's mission. However, CBOT is a mid-size community bank[22] in Texas. While CBOT did have a detrimental impact on

21 FinCEN, Statement on Enforcement of the BSA (Aug. 18, 2020), https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement_FINAL%20508.pdf.

22 The OCC defines "community banks" as banks that typically conduct traditional banking activities and have assets under $8 billion.

FinCEN's mission, the impact appears to have been localized and modest given the Bank's relative size as compared to the rest of the industry.

- Pervasiveness of wrongdoing within the financial institution. CBOT's violations were not the result of pervasive wrongdoing within the organization, although the failures occurred at multiple levels within the organization. Principally, the non-compliance was centered within the AML office, which failed to fully respond to the risks inherent in the Bank's customer base. However, the office's failures were compounded by the Bank's inadequate staffing and oversight of the AML office, either through the BSA Officer, or otherwise.

- History of similar violations or misconduct in general. CBOT has not been the subject of prior criminal, civil, or regulatory enforcement action.

- Presence or absence of prompt, effective action to terminate the violations upon discovery, including self-initiated remedial measures. Once alerted to the violations, CBOT engaged in effective action to terminate the violations. After FinCEN served the bank with a notice of investigation on November 1, 2018, all of CBOT's former AML office employees voluntarily resigned from CBOT and the BSA Officer retired. Thereafter, in late November 2019, CBOT hired a new Director of Financial Crimes with significant experience and expertise to replace the former BSA Officer. The Bank increased AML staffing, including by adding experienced BSA managers, and has undertaken steps to establish on-demand staff augmentation. CBOT conducted a suspicious activity lookback and back-filed 17 SARs since learning of FinCEN's investigation.

- Timely and voluntary disclosure of the violations to FinCEN. CBOT did not voluntarily disclose the violations or its compliance failures to FinCEN.

- Quality and extent of cooperation with FinCEN and other relevant agencies. CBOT formed a Special Committee of the Board of Directors to oversee the Bank's response to FinCEN's investigation, and was responsive to requests for information from FinCEN. CBOT signed multiple agreements tolling the statutes of limitations with FinCEN and the OCC during the course of their investigations.

- Whether another agency took enforcement action for related activity. Following a separate but parallel investigation by the OCC, CBOT has agreed to pay a civil penalty of $1,000,000 ($1 million) for related violations. As many of these violations also form the factual basis for CBOT's BSA violations, FinCEN will credit payments made by CBOT to resolve the OCC's enforcement action.

V. CIVIL PENALTY

FinCEN may impose a Civil Money Penalty of up to $25,000 per day for willful violations of the requirement to implement and maintain an effective AML program occurring on or before November 2, 2015, and up to $59,017 per day for violations occurring after that date.[23]

For each willful violation of a SAR reporting requirement occurring on or before November 2, 2015, FinCEN may impose a Civil Money Penalty not to exceed the greater of the amount involved in the transaction (capped at $100,000) or $25,000.[24] The per-violation cap increases to $236,071, and the floor increases to $59,017, for violations occurring after November 2, 2015.[25]

23 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

24 31 U.S.C. § 5321(a)(1).

25 31 C.F.R. § 1010.821.

After considering all the facts and circumstances, as well as the enforcement factors discussed above, FinCEN is imposing a Civil Money Penalty of $8,000,000 ($8 million) in this matter. As discussed above, FinCEN will credit the $1,000,000 ($1 million) civil penalty imposed by the OCC. Accordingly, CBOT shall make a payment of $7,000,000 ($7 million) to the U.S. Department of the Treasury pursuant to the payment instructions that will be transmitted to CBOT upon execution of this Consent Order.

VI. CONSENT AND ADMISSIONS

To resolve this matter, and only for that purpose, CBOT admits to the Statement of Facts and Violations set forth in this Consent Order and admits that it willfully violated the BSA and its implementing regulations. CBOT consents to the use of the Statement of Facts, and any other findings, determinations, and conclusions of law set forth in this Consent Order in any other proceeding brought by or on behalf of FinCEN, or to which FinCEN is a party or claimant and agrees they shall be taken as true and correct and be given preclusive effect without any further proof. CBOT understands and agrees that in any administrative or judicial proceeding brought by or on behalf of FinCEN against it, including any proceeding to enforce the Civil Money Penalty imposed by this Consent Order or for any equitable remedies under the BSA, CBOT shall be precluded from disputing any fact or contesting any determinations set forth in this Consent Order.

To resolve this matter, CBOT agrees to and consents to the issuance of this Consent Order and all terms herein and agrees to make a payment of $7,000,000 ($7 million) to the U.S. Department of the Treasury within ten (10) days of the Effective Date of this Consent Order, as defined further below. If timely payment is not made, CBOT agrees that interest, penalties, and administrative costs will accrue.[26] If CBOT fails to pay the $1,000,000 ($1 million) penalty arising out of its OCC violations, it must pay the entire $8,000,000 ($8 million) penalty imposed by this Consent Order.

26 31 U.S.C. § 3717; 31 C.F.R. § 901.9.

CBOT understands and agrees that it must treat the Civil Money Penalty paid under this Consent Order as a penalty paid to the government and may not claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for any payments made to satisfy the Civil Money Penalty. CBOT understands and agrees that any acceptance by or on behalf of FinCEN of any partial payment of the Civil Money Penalty obligation will not be deemed a waiver of CBOT's obligation to make further payments pursuant to this Consent Order, or a waiver of FinCEN's right to seek to compel payment of any amount assessed under the terms of this Consent Order, including any applicable interest, penalties, or other administrative costs.

CBOT affirms that it agrees to and approves this Consent Order and all terms herein freely and voluntarily and that no offers, promises, or inducements of any nature whatsoever have been made by FinCEN or any employee, agent, or representative of FinCEN to induce CBOT to agree to or approve this Consent Order, except as specified in this Consent Order.

CBOT understands and agrees that this Consent Order implements and embodies the entire agreement between CBOT and FinCEN, and its terms relate only to this enforcement matter and any related proceeding and the facts and determinations contained herein. CBOT further understands and agrees that there are no express or implied promises, representations, or agreements between CBOT and FinCEN other than those expressly set forth or referred to in this Consent Order and that nothing in this Consent Order is binding on any other law enforcement or regulatory agency or any other governmental authority, whether foreign, Federal, State, or local.

CBOT understands and agrees that nothing in this Consent Order may be construed as allowing CBOT, its holding company, subsidiaries, affiliates, Board, officers, employees, or agents to violate any law, rule, or regulation.

CBOT consents to the continued jurisdiction of the courts of the United States over it and waives any defense based on lack of personal jurisdiction or improper venue in any action to enforce the terms and conditions of this Consent Order or for any other purpose relevant to this enforcement action. Solely in connection with an action filed by or on behalf of FinCEN to enforce this Consent Order or for any other purpose relevant to this action, CBOT authorizes and agrees to accept all service of process and filings through the Notification procedures below and to waive formal service of process.

VII. COOPERATION

CBOT shall fully cooperate with FinCEN in any and all matters within the scope of or related to the Statement of Facts, including any investigation of its current or former directors, officers, employees, agents, consultants, or any other party. CBOT understands that its cooperation pursuant to this paragraph shall include, but is not limited to, truthfully disclosing all factual information with respect to its activities, and those of its present and former directors, officers, employees, agents, and consultants. This obligation includes providing to FinCEN, upon request, any document, record or other tangible evidence in its possession, custody, or control, about which FinCEN may inquire of CBOT. CBOT's cooperation pursuant to this paragraph is subject to applicable laws and regulations, as well as valid and properly documented claims of attorney-client privilege or the attorney work product doctrine.

VIII. RELEASE

Execution of this Consent Order and compliance with all of the terms of this Consent Order settles all claims that FinCEN may have against CBOT for the conduct described in this Consent Order during the Relevant Time Period. Execution of this Consent Order, and compliance with the terms of this Consent Order, does not release any claim that FinCEN may have for conduct by CBOT other than the conduct described in this Consent Order during the Relevant Time Period, or any claim that

FinCEN may have against any current or former director, officer, owner, or employee of CBOT, or any other individual or entity other than those named in this Consent Order. In addition, this Consent Order does not release any claim or provide any other protection in any investigation, enforcement action, penalty assessment, or injunction relating to any conduct that occurs after the Relevant Time Period as described in this Consent Order.

IX. WAIVERS

Nothing in this Consent Order shall preclude any proceedings brought by, or on behalf of, FinCEN to enforce the terms of this Consent Order, nor shall it constitute a waiver of any right, power, or authority of any other representative of the United States or agencies thereof, including but not limited to the Department of Justice.

In consenting to and approving this Consent Order, CBOT stipulates to the terms of this Consent Order and waives:

A. Any and all defenses to this Consent Order, the Civil Money Penalty imposed by this Consent Order, and any action taken by or on behalf of FinCEN that can be waived, including any statute of limitations or other defense based on the passage of time;

B. Any and all claims that FinCEN lacks jurisdiction over all matters set forth in this Consent Order, lacks the authority to issue this Consent Order or to impose the Civil Money Penalty, or lacks authority for any other action or proceeding related to the matters set forth in this Consent Order;

C. Any and all claims that this Consent Order, any term of this Consent Order, the Civil Money Penalty, or compliance with this Consent Order, or the Civil Money Penalty, is in any way unlawful or violates the Constitution of the United States of America or any provision thereof;

D. Any and all rights to judicial review, appeal or reconsideration, or to seek in any way to contest the validity of this Consent Order, any term of this Consent Order, or the Civil Money Penalty arising from this Consent Order;

E. Any and all claims that this Consent Order does not have full force and effect, or cannot be enforced in any proceeding, due to changed circumstances, including any change in law;

F. Any and all claims for fees, costs, or expenses related in any way to this enforcement matter, Consent Order, or any related administative action, whether arising under common law or under the terms of any statute, including, but not limited to, under the Equal Access to Justice Act. CBOT agrees to bear its own costs and attorneys' fees.

X. VIOLATIONS OF THIS CONSENT ORDER

Determination of whether CBOT has failed to comply with this Consent Order, or any portion thereof, and whether to pursue any further action or relief against CBOT, shall be in FinCEN's sole discretion. If FinCEN determines, in its sole discretion, that a failure to comply with this Consent Order, or any portion thereof, has occurred, or that CBOT has made any misrepresentations to FinCEN or any other government agency related to the underlying enforcement matter, FinCEN may void any and all releases or waivers contained in this Consent Order; reinstitute administrative proceedings; take any additional action that it deems appropriate; and pursue any and all violations, maximum penalties, injunctive relief, or other relief that FinCEN deems appropriate. FinCEN may take any such action even if it did not take such action against CBOT in this Consent Order and notwithstanding the releases and waivers herein. In the event FinCEN takes such action under this paragraph, CBOT expressly agrees to toll any applicable statute of limitations and to waive any defenses based on a statute of limitations or the passage of time that may be applicable to the Statement of Facts in this

Consent Order, until a date 180 days following CBOT's receipt of notice of FinCEN's determination that a misrepresentation or breach of this agreement has occurred, except as to claims already time barred as of the Effective Date of this Consent Order.

In the event that FinCEN determines that CBOT has made a misrepresentation or failed to comply with this Consent Order, or any portion thereof, all statements made by or on behalf of CBOT to FinCEN, including the Statement of Facts, whether prior or subsequent to this Consent Order, will be admissible in evidence in any and all proceedings brought by or on behalf of FinCEN. CBOT agrees that it will not assert any claim under the Constitution of the United States of America, Rule 408 of the Federal Rules of Evidence, or any other law or federal rule that any such statements should be suppressed or are otherwise inadmissible. Such statements will be treated as binding admissions, and CBOT agrees that it will be precluded from disputing or contesting any such statements. FinCEN shall have sole discretion over the decision to impute conduct or statements of any director, officer, employee, agent, or any person or entity acting on behalf of, or at the direction of CBOT in determining whether CBOT has violated any provision of this Consent Order.

XI. PUBLIC STATEMENTS

CBOT expressly agrees that it shall not, nor shall its attorneys, agents, partners, directors, officers, employees, affiliates, or any other person authorized to speak on its behalf or within its authority or control, take any action or make any public statement, directly or indirectly, contradicting its admissions and acceptance of responsibility or any terms of this Consent Order, including any fact finding, determination, or conclusion of law in this Consent Order.

FinCEN shall have sole discretion to determine whether any action or statement made by CBOT, or by any person under the authority, control, or speaking on behalf of CBOT contradicts this Consent Order, and whether CBOT has repudiated such statement.

XII. RECORD RETENTION

In addition to any other record retention required under applicable law, CBOT agrees to retain all documents and records required to be prepared or recorded under this Consent Order or otherwise necessary to demonstrate full compliance with each provision of this Consent Order, including supporting data and documentation. CBOT agrees to retain these records for a period of six years after creation of the record, unless required to retain them for a longer period of time under applicable law. FinCEN and CBOT agree that any electronic records generated by or through the automated transaction monitoring system the Bank used during the Relevant Time Period need not be retained past May 1, 2025.

XIII. SEVERABILITY

CBOT agrees that if a court of competent jurisdiction considers any of the provisions of this Consent Order unenforceable, such unenforceability does not render the entire Consent Order unenforceable. Rather, the entire Consent Order will be construed as if not containing the particular unenforceable provision(s), and the rights and obligations of FinCEN and CBOT shall be construed and enforced accordingly.

XIV. SUCCESSORS AND ASSIGNS

CBOT agrees that the provisions of this Consent Order are binding on its owners, officers, employees, agents, representatives, affiliates, successors, assigns, and transferees to whom CBOT agrees to provide a copy of the executed Consent Order. Should CBOT seek to sell, merge, transfer, or assign its operations, or any portion thereof, that are the subject of this Consent Order, CBOT must, as a condition of sale, merger, transfer, or assignment obtain the written agreement of the buyer, merging entity, transferee, or assignee to comply with this Consent Order.

XV. MODIFICATIONS AND HEADINGS

This Consent Order can only be modified with the express written consent of FinCEN and CBOT. The headings in this Consent Order are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Order or its individual terms.

XVI. AUTHORIZED REPRESENTATIVE

CBOT's representative, by consenting to and approving this Consent Order, hereby represents and warrants that the representative has full power and authority to consent to and approve this Consent Order for and on behalf of CBOT, and further represents and warrants that CBOT agrees to be bound by the terms and conditions of this Consent Order.

XVII. NOTIFICATION

Unless otherwise specified herein, whenever notifications, submissions, or communications are required by this Consent Order, they shall be made in writing and sent via first-class mail and simultaneous email, addressed as follows:

To FinCEN: Associate Director, Enforcement and Compliance Division, Financial Crimes Enforcement Network, P.O. Box 39, Vienna, Virginia 22183

To CBOT: Justin Long
Senior Executive Vice President and General Counsel
CommunityBank of Texas, N.A.
9 Greenway Plaza, Suite 110
Houston, Texas 77046

Notices submitted pursuant to this paragraph will be deemed effective upon receipt unless otherwise provided in this Consent Order or approved by FinCEN in writing.

XVIII. COUNTERPARTS

This Consent Order may be signed in counterpart and electronically. Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

XIX. EFFECTIVE DATE AND CALCULATION OF TIME

This Consent Order shall be effective upon the date signed by FinCEN. Calculation of deadlines and other time limitations set forth herein shall run from the effective date (excluding the effective date in the calculation) and be based on calendar days, unless otherwise noted, including intermediate Saturdays, Sundays, and legal holidays.

By Order of the Director of the Financial Crimes Enforcement Network.

/s/

Himamauli Das
Acting Director

Date:

Consented to and Approved By:

/s/

Robert R. Franklin, Jr.
Chairman and Chief Executive Officer
CommunityBank of Texas, N.A.