

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

**IN THE MATTER OF:**

)

)

**Bank of America, N.A.**

)

**Number 2026-03**

**CONSENT ORDER IMPOSING CIVIL MONEY PENALTY**

The Financial Crimes Enforcement Network (FinCEN) has conducted a civil enforcement investigation and determined that grounds exist to impose a Civil Money Penalty against Bank of America, N.A. (Bank of America or the Bank) for violations of the Bank Secrecy Act (BSA) and its implementing regulations.<sup>1</sup> Bank of America admits to the Statement of Facts and Violations set forth below, consents to the issuance of this Consent Order, agrees to pay the civil money penalty imposed in this Consent Order, and agrees to comply with the provisions of this Consent Order, including, but not limited to, the Undertakings.

**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.<sup>2</sup>

At all times relevant to this Consent Order, Bank of America was a “bank” and a “domestic financial institution” as defined by the BSA and its implementing regulations.<sup>3</sup> As such, Bank of America was required to comply with applicable BSA regulations.

---

<sup>1</sup> The BSA is codified at 12 U.S.C. §§ 1829b, 1951-1960, 31 U.S.C. §§ 5311-5314, 5316-5336 and includes other authorities reflected in notes thereto. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.

<sup>2</sup> 31 U.S.C. § 5321(a); 31 C.F.R. § 1010.810(a), (d); Treasury Order 180-01 (July 1, 2014, reaff’d Jan. 14, 2020).

<sup>3</sup> 31 U.S.C. § 5312(a)(2), (b)(1); 31 C.F.R. § 1010.100(d), (t)(1).

AML Program: The BSA and its implementing regulations require U.S. banks, such as Bank of America, to implement and maintain an anti-money laundering (AML) program, including policies, procedures, and controls to assure ongoing compliance with the applicable provisions of the Bank Secrecy Act.<sup>4</sup> Bank of America is also required to: (i) conduct independent testing for compliance; (ii) designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance; (iii) conduct ongoing training for appropriate persons; and (iv) implement appropriate risk-based procedures for conducting ongoing customer due diligence (CDD), including but not limited to (a) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile and (b) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.<sup>5</sup>

Due Diligence on Correspondent Accounts for Foreign Financial Institutions: The BSA and its implementing regulations require all “covered financial institutions,” including banks such as Bank of America, to establish a due diligence program that includes appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to enable the covered financial institution to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed by such covered financial institution in the United States for a foreign financial institution.<sup>6</sup>

---

<sup>4</sup> 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210.

<sup>5</sup> 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210(a). These are often referred to as the five “pillars” of a bank’s AML program.

<sup>6</sup> 31 U.S.C. § 5318(i); 31 C.F.R. § 1010.610.

FinCEN's regulations require that such due diligence programs include specific requirements, specifically: (i) determining whether any such correspondent account is subject to enhanced due diligence; (ii) assessing the money laundering risk presented by such correspondent account, based on a consideration of all relevant factors, which shall include, as appropriate: (a) the nature of the foreign financial institution's business and the markets it serves, (b) the type, purpose, and anticipated activity of such correspondent account, (c) the nature and duration of the covered financial institution's relationship with the foreign financial institution (and any of its affiliates), (d) the AML and supervisory regime of the jurisdiction that issued the charter or license to the foreign financial institution, and, to the extent that information regarding such jurisdiction is reasonably available, of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered, and (e) information known or reasonably available to the covered financial institution about the foreign financial institution's anti-money laundering record; and (iii) applying risk-based procedures and controls to each such correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity sufficient to determine consistency with information obtained about the type, purpose, and anticipated activity of the account.<sup>7</sup>

Suspicious Activity Reporting: A bank must identify suspicious transactions relevant to a possible violation of law or regulation in suspicious activity reports (SARs) filed with FinCEN.<sup>8</sup> Specifically, the BSA and its implementing regulations require banks to report transactions that involve or aggregate to at least \$5,000, are conducted or attempted by, at, or through the bank, and

---

<sup>7</sup> 31 C.F.R. § 1010.610(a).

<sup>8</sup> 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320.

that the bank “knows, suspects, or has reason to suspect” are suspicious.<sup>9</sup> A transaction is “suspicious” if a bank “knows, suspects, or has reason to suspect” the transaction: (i) involves funds derived from illegal activities, or is intended or conducted to disguise funds derived from illegal activities as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation; (ii) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations implementing it; or (iii) 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.<sup>10</sup> 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.<sup>11</sup>

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.<sup>12</sup>

## **II. STATEMENT OF FACTS**

The conduct described below took place from at least January 1, 2018 through July 1, 2025 (the Relevant Time Period) unless otherwise indicated.

---

<sup>9</sup> *Id.*

<sup>10</sup> 31 C.F.R. § 1020.320(a)(2).

<sup>11</sup> 31 C.F.R. § 1020.320(b)(3).

<sup>12</sup> FINCEN, FIN-2014-A007, [FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance](#) (Aug. 11, 2014).

### **A. 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 violations of the BSA.<sup>13</sup> As 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).<sup>14</sup>

### **B. 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.<sup>15</sup> Under this authority, the OCC conducts regular examinations and issues reports assessing a bank’s compliance with the BSA and other requirements.

### **C. Bank of America, N.A.**

Bank of America is the primary bank subsidiary of Bank of America Corporation, a financial holding company based in Charlotte, North Carolina and incorporated in Delaware whose shares are publicly traded on the New York Stock Exchange under the ticker symbol “BAC.” Bank of America is the second largest bank in the United States, with roughly \$2.7 trillion in total assets,

---

<sup>13</sup> 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. Bank of America admits to “willfulness” only as the term is used in civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1).

<sup>14</sup> 31 C.F.R. § 1010.810(a), (d).

<sup>15</sup> *Id.*; 12 U.S.C. § 1818(s)(2); 12 C.F.R. § 21.21.

and is also a “global systemically important bank.”<sup>16</sup> Bank of America provides banking, investment, mortgage, trust, and payment services to individuals, businesses, local governments, and other financial institutions. The Bank employs approximately 211,000 personnel and maintains over 3,500 branches and approximately 15,000 ATM locations in the United States. The Bank’s most recent annual financial disclosure reported net income of approximately \$30.5 billion.

#### **D. Bank of America Failed to Implement and Maintain an AML Program**

Bank of America willfully failed to implement and maintain an AML program that met several of the BSA’s requirements during the Relevant Time Period. The Bank’s failures, described below, related to several regulatory requirements (commonly referred to as “pillars”) of the AML program.

The Bank willfully failed to implement and maintain adequate internal controls for BSA compliance, primarily due to critical deficiencies and gaps in its proprietary transaction monitoring system, which resulted in both missed and delayed detection and reporting by Bank of America of *over \$5 billion of suspicious activity, with roughly \$1 billion of this activity implicating national security-related and other priority illicit finance risks, including suspicious transactions indicative of Chinese Money Laundering Networks (CMLNs), fraud, and potential trade-based money laundering (TBML) with a substantial nexus to the southwest border*. Further, Bank of America’s AML program deficiencies extended to its CDD procedures, including for high-risk customers that operated in the online auto auction industry, further contributing to such unreported or untimely reported suspicious activity.

---

<sup>16</sup> FINANCIAL STABILITY BOARD, [2025 List of Globally Systemically Important Banks](#) (Nov. 27, 2025).

These violations generally continued throughout the Relevant Time Period despite repeated internal warnings from the Bank's own personnel performing compliance and testing functions as well as external concerns raised by law enforcement and other financial institutions.

### **1. Inadequate Internal Controls**

Throughout the Relevant Time Period, Bank of America willfully failed to implement and maintain a system of internal controls sufficient to assure the Bank's ongoing compliance with the BSA and its implementing regulations. This resulted from several issues related to the design and implementation of Bank of America's proprietary transaction monitoring system, Event Processor (EP), the primary control that the Bank used to fulfill its obligation to identify and report suspicious activity. As further detailed in Section II.F, *infra*, these issues meant the Bank did not report large volumes of suspicious activity implicating national security-related and other priority illicit finance risks, including over \$600 million of transactions with indicia of potential TBML involving salvaged vehicles (roughly one-third of which had a nexus to the southwest border) and hundreds of millions of dollars of transactions consistent with a CMLN typology.

The issues with EP resulted in the Bank *relying upon law enforcement, other financial institutions, and internal manual referral processes* to identify and report suspicious activity: *for multiple years within the Relevant Time Period, more than one-third of Bank of America's suspicious activity investigations were prompted by such events<sup>17</sup> instead of the Bank's own automated, internal controls*, and as described below, such reliance appears to have occurred at least in part due to gaps and deficiencies in EP (*e.g.*, with respect to certain online auto auction customers posing an elevated risk of money laundering, the vast majority of case investigations

---

<sup>17</sup> As explained below, these events were identified in EP as "promotion" events, which related documentation described as "events that contain human intelligence . . . such as Manual Referrals . . . Law Enforcement Referrals, 314(a) [requests], 314(b) [requests], and Grand Jury Subpoenas." The Bank's metrics related to EP often identified a substantial portion of such "human intelligence" cases as being attributed to "external events."

resulted from the Bank’s receipt of external requests rather than EP’s generation of alerts on a risk basis). Additionally, the Bank filed a *material portion of its SARs more than six months after the relevant activity took place* in accordance with EP processes, which aggregated activity—often for extended periods of time—to determine if such activity was suspicious.

After making adjustments to core aspects of EP—including the threshold levels—in December 2023 (which followed engagement with regulators), Bank of America conducted a *one-time, limited scope lookback that identified nearly \$4 billion in suspicious activity* that would not have otherwise been timely investigated and reported under EP’s thresholds in place for the majority of the Relevant Time Period. Because EP consolidated considerable activity before any human investigation occurred, the Bank’s investigators were, at times, unable to conduct a meaningful review of the relevant activity, which resulted in *SARs that failed to provide FinCEN with a complete report of the customer’s suspicious transactions*.

Bank of America began taking steps to address the various issues with EP after extensive engagement with its prudential regulators (and after FinCEN commenced its investigation) about deficiencies and gaps in EP as well as other aspects of its AML/CFT program. However, the issues with EP remained unresolved as recently as June 2025, when, as required by one of the Bank’s prudential regulators, a third party issued a report, which included several findings related to EP consistent with those identified in FinCEN’s investigation.

As detailed below, FinCEN’s investigation identified the following primary issues with EP: (i) the Bank’s design choices for core aspects of EP lacked empirical support that resulted in EP being insufficiently grounded in the risks that Bank of America faced, as well as triggering investigations of potentially suspicious activity well after—and, in some cases, more than a year after—the relevant transactions took place; (ii) the Bank failed to meaningfully update key aspects

of EP during the Relevant Time Period; (iii) the Bank failed to adequately respond to testing indicating that core aspects of EP—including the primary threshold used to determine whether an alert of potentially suspicious activity generated a case for investigation—were ineffective in facilitating Bank of America’s compliance with its obligation to identify and report suspicious transactions; (iv) the Bank added rules within EP to “rescore” or “suppress” activity that resulted in such activity being not investigated or subject to delayed investigation without sufficient governance and oversight processes to ensure the risk-based application of these rules;<sup>18</sup> and (v) EP included only limited coverage of large volumes of negotiable instrument deposit activity, despite the Bank being aware that certain higher-risk customers were engaged in patterns of suspicious transactions involving this product, as well as failed to include in EP appropriate monitoring of credit card activity.

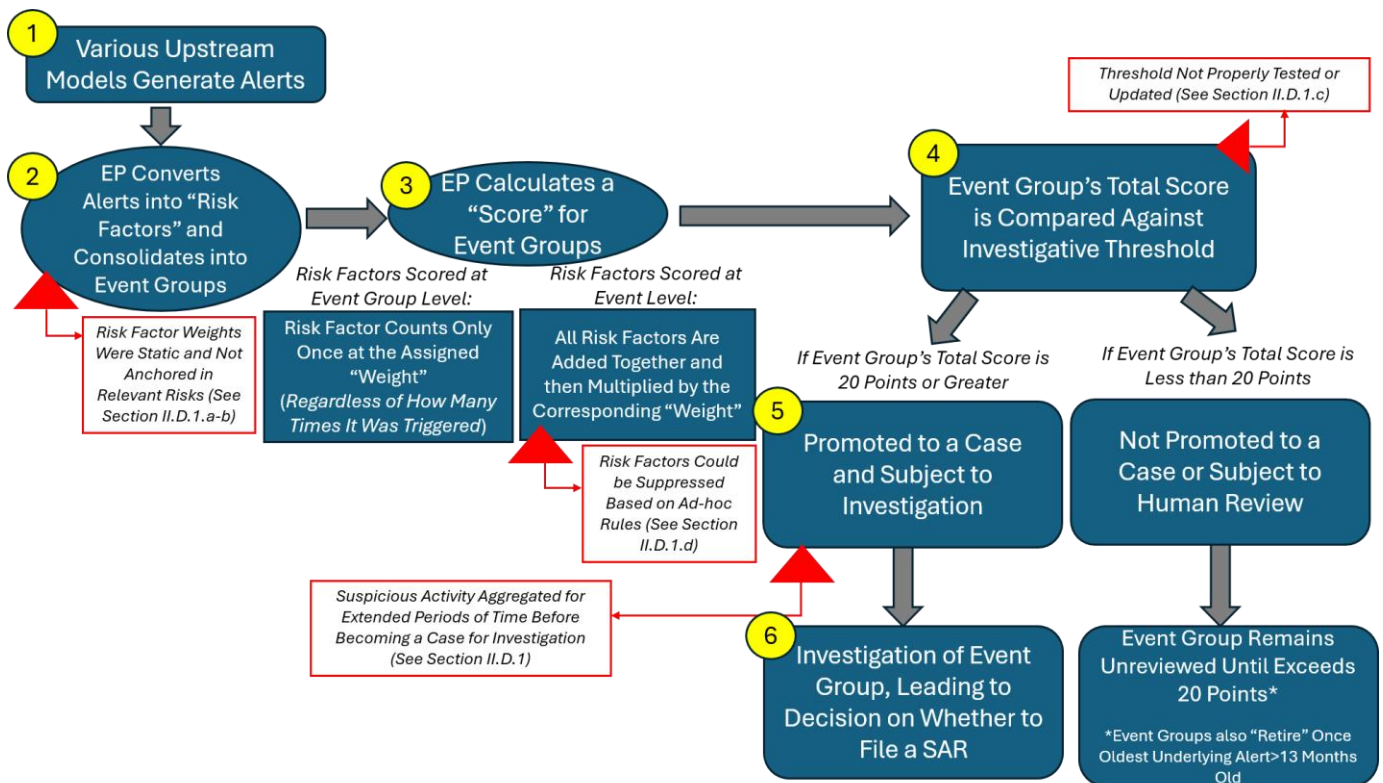
***Background on Event Processor.*** In 2010, Bank of America designed and, through a “proof of concept,” first implemented EP to manage the Bank’s transaction monitoring alerts of potentially suspicious activity. Bank of America designed EP to act as an interconnected model system, the main objectives of which were the monitoring, identifying, investigating, and reporting of suspicious activity. The Bank’s records described EP as the first of its kind in the industry, with “very little documentation or literature to draw from in its creation.” EP was created to solve challenges associated with reviewing alerts associated with individual transactions, including that “there were ***not enough investigators to work all of the alerts that were being generated*** by detection channels.”<sup>19</sup>

---

<sup>18</sup> Bank of America’s documentation of these features within EP used the terms “rescore” and “suppress” interchangeably.

<sup>19</sup> Unless otherwise indicated, bold and italicized text within a quotation reflects emphasis added.

As designed, EP resulted in individual alerts of potentially suspicious activity associated with a transaction (referred to by the Bank as “events”) generally not being subject to manual review by an investigator. Instead (and as depicted in the graphic below),<sup>20</sup> EP individually assigned a weighted score to each alert by assigning the alert “risk factors” and consolidated—generally at the customer level—the alerts generated within a defined time period (described below) into groups (Event Groups). Event Groups consisted of all individual alerts associated with a customer within a defined time period (described below), with the weighted risk score assigned to these alerts combined to generate a risk score for the Event Group as a whole. Absent auto-promotion (as described below), an Event Group generally would not be subject to investigation until its combined risk score reached a threshold score of 20 points. This threshold, “initially set by stakeholder judgment,” remained in place until December 2023.



<sup>20</sup> The graphic represents a simplified visualization of EP based on FinCEN’s investigation of the system.

During the Relevant Time Period, EP included hundreds of risk factors that ranged in weights from 0 to 20 points. Risk factors were configured to apply at the event group, event, party, and account levels and were processed two times each weekday. EP's inclusion of "Event Group level" risk factors meant that such risk factors contributed only once to the Event Group's total score, irrespective of how many times the associated alert had been triggered. For example, one of the alerts in effect during the Relevant Time Period involved certain large aggregated incoming wires for the relevant customer that was assigned a weight of 1 point within EP, but because EP calculated this as an Event Group level score, no matter how many times this alert generated, it could only ever contribute 1 point to the relevant Event Group.

By contrast, many risk factors were scored at the "event level," meaning their score counted towards the Event Group score each time the risk factor was triggered. The Bank's documentation on EP noted that this summation of scores within an Event Group was selected "as the simplest way to combine weights for disparate detection channels," but also acknowledged that "detection channels could interact in a non-linear fashion." In other words, because EP's design allowed for a large amount of potentially suspicious activity to accumulate within an Event Group before it would be subject to investigation, various different types of potentially suspicious activity could combine within the Event Group and result in that Event Group accumulating risk at a much faster rate than the risk weights of its individual component alerts—even if properly calibrated on an individual basis—would suggest.

In order for a case to be created and thereby trigger review by a Bank investigator, the Event Group must have reached the threshold score of 20 points within 13 months of the oldest active alert within the Event Group, with any alerts (other than those that formed an Event Group already subject to investigation) older than 13 months subject to "retirement," such that they would

still be included in the Event Group, but no longer contribute to that Event Group's total score. The Event Group, however, would continue to generate new alerts so long as it contained at least one alert that was less than 13 months old.

The 13-month window was chosen based on "stakeholder judgment" to "ensure that all activity within a full calendar year would be considered," as Bank of America believed that a larger window "increases the probability that a few false positive[s] . . . might combine to reach the case [creation] threshold." However, as detailed below, many risk weights were not appropriately calibrated to reflect the relevant risks; as a result, many cases that would have resulted in SARs never reached the 20-point threshold within this timeframe.

Once an Event Group received a score of 20 points, it formed a "case" that was sent to an AML investigator for manual review. One of the ways that an Event Group could reach this threshold was through what the Bank deemed to be "auto-promote" events that automatically caused an Event Group to form a case subject to review by an investigator, a material portion of which were based on "external events" occurring outside EP, such as the Bank's receipt of seizure warrants or a subpoena. As noted above, FinCEN's investigation found that, for several years within the Relevant Time Period, this "auto promotion" feature of EP contributed to more than one-third of all investigations that the Bank conducted in a given year.

The Bank performed regular evaluations of EP to determine if EP identified all activity that it should have been identifying and ensure that EP was prioritizing alerted activity in accordance with its attendant risk. However, as detailed below, the testing was inadequate because, among other things, it did not focus on whether EP was appropriately capturing Bank of America's risk, and even where such testing did highlight issues with EP, the Bank failed to reasonably address such issues.

Following engagement with the Bank’s prudential regulators, in December 2023, Bank of America lowered the 20-point threshold to either 10 or 12 points depending on certain characteristics of the Event Group. After the Bank’s risk analytics team completed its analysis following these changes, the Bank “found that the new thresholds...are deemed to be reasonable, given that the new thresholds can capture the majority of the SAR-worthy alerts across scenarios.” Bank of America also decreased the time that Event Groups remain open from 13 months to four months<sup>21</sup> and introduced certain false negative thresholds, including a 5% tolerance level for false negatives for purposes of management oversight,<sup>22</sup> whereas there previously had been no predefined tolerance level. In 2024, Bank of America conducted a one-time lookback for potential missed suspicious activity under these revised parameters for EP and ***found that under the revised thresholds, the Bank had failed to identify and file nearly 8,900 SARs, with transaction activity totaling nearly \$4 billion.*** Further, in connection with the implementation, the Bank estimated that the revised threshold would result in an ***increase of 16,000 U.S. investigations each month,*** representing “double [the] prior ongoing monthly volume” and requiring the Bank to increase staffing with an ***“incremental 750” personnel*** to support such volumes going forward (in addition to 800 consultants required to complete the one-time lookback).

In 2024, a planning document for a new approach to transaction monitoring stated that the case creation process under consideration would streamline this “process from the prior overly complex Event Processor model to a transparent, rule-based case escalation logic.” This 2024

---

<sup>21</sup> As described below in Section II.D.1.c, even after the threshold was lowered in 2023, the Bank failed to identify and timely report a significant amount of illicit activity, such as suspicious transactions with indicia of CMLNs.

<sup>22</sup> Bank of America also introduced a 7.5% false negative tolerance threshold for further escalation to the Board. Since 2026, the Bank has replaced these thresholds with lower and more granular thresholds for activity that relates to FinCEN’s National Priorities and other criminal-related typologies with activity over \$500,000.

planning document addressed issues associated with planning and adaptation of EP over its lifespan.

In December 2024, the OCC issued a Cease-and-Desist Order against Bank of America for BSA deficiencies, which included the requirement to conduct a validation of and lookback related to the Bank's transaction monitoring system.<sup>23</sup> Subsequent independent testing conducted by a third party in 2025 observed continued critical findings related to Bank of America's approach to transaction monitoring and ongoing issues with EP.

#### **a) Risk Weights Not Properly Calibrated for Attendant Risks**

As detailed below, many of EP's risk factor weights were largely unsubstantiated and were not sufficiently anchored in relevant risks. An internal "Performance Analysis" report on EP issued in April 2019, described, among other aspects of EP, a risk factor for the ATM Large Cash Deposit Model that required five conditions to trigger an alert. The report found that the necessity to fulfill all five conditions was a "very strict requirement" and that a "study of SAR case narratives from 2016 to 2018 found that SARs could be filed even when only one condition...was satisfied. In other words, it might not be necessary to require all five conditions to be satisfied at the same time." Moreover, the report observed that *this risk factor was weighted only one point in EP, but the Bank's own testing had found that this risk factor had a SAR yield of 56.75%.*<sup>24</sup>

---

<sup>23</sup> OFFICE OF THE COMPTROLLER OF THE CURRENCY, [\*OCC Issues Cease and Desist Order Against Bank of America for BSA Deficiencies\*](#), (Dec.23, 2024).

<sup>24</sup> SAR yield refers to the percentage of SARs the Bank files that result from the total number of Event Groups containing a certain risk factor or AML model in EP. As detailed below. Bank of America used SAR yield to measure the effectiveness of various aspects of EP, including risk factor weights as well as EP's 20-point investigative threshold. However, having identified SAR yield as an important metric for assessing EP's effectiveness, the Bank failed to take appropriate action when testing identified issues with EP, such as risk factor weights that were too low relative to their SAR yield. Banks and other financial institutions may find it useful to measure SAR yield in evaluating the effectiveness of their internal controls, but this is not the only metric that can be considered. Additionally, when assessing SAR yield or other potential metrics to evaluate internal control effectiveness, the financial institution should consider how to apply such metrics to the financial institution's risk profile, including how it may evolve over time. In this example, more than half of the alerts generated by the ATM Large Cash Deposit Model resulted in the Bank identifying suspicious activity and filing a SAR.

Similarly, a 2022 “Model Validation Report” of EP contained a table that compared the “relative feature importance, the risk factor weights, and the corresponding SAR Yields” of each risk factor. Several of the risk factors that this table highlighted as having the highest “feature importance” in EP’s ability to identify suspicious activity, such as “High Intensity Drug Trafficking Area (HIDTA)<sup>25</sup>” and “cash structuring,” had ***EP risk factor weights of only 1 point, but SAR yields above 50%***. Even assuming that such alerts eventually became part of an Event Group that reached the relevant threshold, the low weights for these risk factors in EP extended the time for an alert to contribute to a case, thereby at least causing delays in the Bank’s detection of relevant suspicious activity.

Testing conducted by Bank of America also demonstrated that differences in risk factor weights were not correlated to their relative SAR yields. An April 2020 report assessed EP’s risk factor weights for a group of 14 types of alerts that related to large wires and highlighted a lack of correlation of the risk factor weights assigned to these 14 types of alerts relative to their associated SAR yields. Among these 14 types of alerts, ***one that produced a SAR yield of 30.03% received a weight in EP of 6 points***, whereas another type of alert with ***a similar SAR yield of 27.69% was assigned a weight in EP of only 2 points***; the report did not discuss why these alerts with similar SAR yields had materially different weights. The report found that yet another of these alerts with a weight of only 2 points had a “relatively large case number and high SAR yield,” so ***its risk weight may have important impact on the performance of this model***,” the report noted that “it may be worth [*sic*] to study whether the performance of this model can be improved by increasing the risk weight of [the risk factor].” Despite the report’s recommendation, this type of alert

---

<sup>25</sup> The High Intensity Drug Trafficking Areas (HIDTA) program, created by Congress with the Anti-Drug Abuse Act of 1988, provides assistance to Federal, state, local, and tribal law enforcement agencies operating in areas determined to be critical drug-trafficking regions of the United States. DEA <https://www.dea.gov/operations/hidta>.

continued to be assigned a weight of 2 points through 2022, with an increase to only 2.5 points in 2023.

The same April 2020 report reviewed alerts generated by an Online Transaction Monitoring-Peer-to-Peer model that the Bank had enhanced in September 2016. Analyzing data from 2017 to 2019, the April 2020 report found that the number of alerts generated by this model increased by the millions every year, but only a small percentage of these ever became cases because the vast majority of them “retired” after 13 months. This April 2020 report observed that these alerts had weights of only 1 or 2 points, but SAR yields above 40% and called out “*the need for a comprehensive review of the current risk score assignment framework.*”

A 2022 validation report also identified similar concerns with the discrepancy between the weights of risk factors and the SAR yields.

#### **b) Risk Factors Not Sufficiently Calibrated, Tested, or Updated Over Time**

Risk factor weights in EP remained static over much of the Relevant Time Period, further contributing to a disconnect between EP and the Bank’s risk profile. From 2018 to 2023, *76% of all risk factor weights remained the same, while the relatively few risk factor weights that changed tended to result in weight reductions: of the roughly 25% of risk factor weights that experienced a change within this timeframe, approximately 80% of such changes were decreases to the risk factor weight.* Even when Bank of America was aware that risk factors needed increased weights, the Bank was delayed in recalibrating and changing these risk factors. Some of these delays were also attributed to the ineffectiveness of the Bank’s internal testing and recommendations.

For example, as mentioned above, *many cash-related risk factors had weights of one point but SAR yields above 50%.* For the model “ATM Large Cash Deposit,” a 2019 report found that

***“the current weights do not align with the high SAR yield.”*** The report acknowledged that Bank of America had added four new risk factors to this model during the most recent model enhancement, but the report also found that ***“all four risk factors have high SAR yields, but each of them only carries a risk weight of 1-pt.”*** The weights associated with these four types of alerts remained unchanged through 2024.

Additionally, the April 2020 report found that certain types of alerts in a cash structuring model with risk factor weights of only 1 or 2 points had high SAR yields, even after enhancement of the model. The report’s accompanying recommendation about these risk factors described the model’s performance as having “improved significantly” and recommended that the Bank monitor the performance of one type of alert generated by this model that did not have a high SAR yield. This report did not include a recommendation to address the low risk factor weights for the many other types of alerts generated by this model that were found to have had high SAR yields.

In late 2021, and in response to certain of the recommendations in these reports, Bank of America published a report summarizing a “Risk Factor Calibration Model” for the weights of risk factors within EP. However, this work was informed by the Bank’s continued focus on improving SAR yield without proper consideration of the risks involved. For example, an internal presentation indicated the model was needed to “calibrate [risk factors] so the whole system of weights has a better SAR yield.” Consistent with this view, the new model resulted in ***“case load reduction,” with the model reducing by over 8,200 the number of cases that would require investigation.*** The report went on to describe the associated “SAR loss” with this “case load reduction” as “permissible,” but did not explain how permissibility was determined.

The recalibration model was also affected by the Bank’s lack of sufficiently objective benchmarks for EP. For example, the Bank had not established a “false negative” tolerance for

EP, so even though the model purported to incorporate a “severe penalization” for false negatives (one of the attributes that the accompanying literature contemplated would be “determined by” the “model owner”), no objective benchmark existed to evaluate the reasonableness of this aspect of the model.

The literature accompanying this 2021 calibration model included a summary table indicating that, in the aggregate, the model’s application *resulted in weight decreases to 106 risk factors in EP while producing increases to 17 risk factors, with the model generating a net decrease of 187 points across the weights of all risk factors in EP*. Among the risk factors whose weights decreased were certain risk factors that prior Bank testing reports had identified as exhibiting a disconnect due to the accompanying high SAR yields. For example, of the seven risk factors associated with the cash structuring that the April 2020 report had identified as having SAR yields of 50% or higher, application of the 2021 calibration model resulted in *decreases* to the weights associated with five of these seven risk factors, with the model’s impact across all seven of these risk factors reflecting an overall weight decrease of seven total points.

The Bank’s testing found that the risk factor weights still failed to properly reflect the relevant risks, even after the development of the “recalibration” model in 2021. A 2022 internal report of a model validation on EP performed by Bank personnel described the weights for some EP risk factors as “counterintuitive” given their low weights versus the high SAR yields.

Bank of America took some action as a result of the 2022 model validation report, but these actions were insufficient to address the pervasive discrepancies with risk factor weights in EP. In May 2022, EP’s model team responded to a model validation “required action item” to investigate why certain risk factors with high SAR yields were assigned lower weights. The response stated that some risk factors were “redundant and exhibit overlapping coverage.” The model team

suggested reducing the weight on secondary risk factors to “improve the overall SAR yield.” This response to the model validation finding focused on optimizing SAR yield, without consideration of a metric for appropriate SAR yields as determined by the Bank’s risk-based approach.<sup>26</sup> This response also did not address findings detailed above of incongruous risk factor weightings in several previous tests of EP.

In 2025, the report of the third party’s review of EP found issues with the risk factor weights in EP: “underweighted risk factors also appear to contribute to higher concentrations of risk in Event Groups with lower scores in EP.” This report specifically reviewed alerts associated with “ATM Large Cash Deposits,” which resulted in a SAR yield more than twice the Bank’s recently implemented tolerance level for “false negatives,” “*indicating an unacceptable level of missed SARs associated with this activity*.” In fact, the risk factor weights for four of these risk factors related to ATM large cash deposits had *decreased* between 2018 and 2024. In sum, Bank of America’s failure to appropriately weight its risk factors, even after testing raised concerns about risk factor weights, caused failures and delays in identifying and reporting suspicious activity, as Event Groups often lingered below the 20-point threshold or expired within the 13-month timeframe to become a case that triggered a Bank investigation.

### **c) Internal Testing Identified Deficiencies With the 20-Point Threshold**

The 20-point threshold for Event Groups to trigger review by the Bank’s investigators was also developed based on “stakeholder judgement” and was not adequately supported by documentation or empirical evidence that such a threshold sufficiently mitigated Bank of America’s risks. As detailed below, multiple tests demonstrated that the Bank failed to investigate

---

<sup>26</sup> As a related example, in describing two risk factors that each related to a customer receiving cash in and sending out a wire, the response stated that one factor “without [the second factor’s] presence. . .has a *poor SAR yield of 44%*.” The response includes no explanation as to why a SAR yield of 44%—which is between roughly 6 and 8 times the objective benchmark for missed suspicious activity that the Bank would later introduce—was considered “poor.”

a material amount of suspicious activity just below the threshold, with this amount of missed activity increasing over time. Despite these results, the Bank reduced this threshold only following extensive engagement with Bank of America’s prudential regulators.

A contributing factor to this inaction was the Bank’s approach to testing EP’s 20-point threshold, which testing generally focused on whether there was a statistically significant difference between the SAR yield above and below the 20-point threshold without taking into account the implications of the suspicious activity being missed or the increasing amount of such activity that the testing identified over time. Moreover, the Bank failed to establish an objective benchmark (e.g., a “false negative” tolerance for suspicious activity not being timely identified) to help inform this testing and provide a standard against which to measure the appropriateness of the 20-point threshold. As detailed in the examples below, the determination of *whether potentially suspicious activity warranted investigation varied from year-to-year, with no explanation of this variability.*

The graphic below depicts Bank of America’s testing of EP’s performance from 2018 to 2020, which consistently found the SAR yield for Event Groups with 20-24 points (*i.e.*, those either *at or just above* the threshold triggering investigation) was roughly 33-34%, but, as the graphic also indicates, the Bank’s subsequent testing of EP’s performance in 2022 and the first quarter of 2023 found that the SAR yield for Event Groups with 16 to 19 points (*i.e.*, those *just below* the threshold that would trigger investigation) were generally between 38% and 45%—not only did this range reflect a substantial increase compared to the testing of these same Event Group scores from 2018 to 2020, but this range was also materially higher than what the Bank had previously found warranted investigation.

|                                                  |                             | SAR Yield 2018-2019 | SAR Yield 2019-2020 |
|--------------------------------------------------|-----------------------------|---------------------|---------------------|
| Event Groups <b>NOT</b> Subject to Investigation | Event Groups – 16 Points    | 22.22%              | 27.98%              |
|                                                  | Event Groups – 17 Points    | 25.26%              | 29.24%              |
|                                                  | Event Groups – 18 Points    | 25%                 | 30.44%              |
|                                                  | Event Groups – 19 Points    | 31.67%              | 31.57%              |
| Event Groups Subject to Investigation            | Event Groups – 20-24 Points | 33.90%              | 34.38%              |



|                          | SAR Yield Q1 2022 | SAR Yield Q2 2022 | SAR Yield Q3 2022 | SAR Yield Q4 2022 | SAR Yield Q1 2023 |
|--------------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| Event Groups – 16 Points | 38.73%            | 38.64%            | 40%               | 38.33%            | 41.79%            |
| Event Groups – 17 Points | 40.95%            | 40.74%            | 33.96%            | 31.34%            | 32.21%            |
| Event Groups – 18 Points | 43.2%             | 42.87%            | 37.5%             | 33.59%            | 31.51%            |
| Event Groups – 19 Points | 45.49%            | 45.03%            | 44.16%            | 44.72%            | 41.41%            |

 Event Group not subject to investigation despite SAR yield being higher than Event Groups that warranted investigation in both 2018-2019 and 2019-2020

Notably, the SAR yields observed throughout 2022 and the first quarter of 2023 for Event Groups with 16 to 19 points were *roughly seven-to-nine times higher than* the “false negative” tolerance of 5% that the Bank would belatedly establish near the end of the Relevant Time Period.

Recommendations made in the testing reports failed to substantively address these SAR yield-related discrepancies or acknowledge the need to consider other interim controls to address the increasing SAR yields for Event Groups under the 20-point threshold.

Several testing reports included certain observations that the SAR yield for Event Groups below the 20-point threshold was not, in fact, statistically different from the 20-point threshold. For example, a report on EP’s performance in 2018 to 2019 found that Event Groups with points “14-19 ha[ve] the highest SAR yield among all strata this year.” The report further stated that this same finding was true of the previous two years, and “the estimated SAR yield of this score group has displayed an increasing trend since 2016.” Similarly, a testing report covering EP’s

performance in 2019 and 2020 found that the SAR yields for Event Groups with risk scores of 18 and 19 (*i.e.*, just below the threshold that would trigger the Bank to investigate the activity) were higher than the SAR yields for Event Groups with risk scores of 20 or 21.

In 2022, Bank of America responded to testing findings, including conducting additional threshold testing of certain models. However, the validation of EP, which culminated in the issuance of a final validation report in 2022—more than a decade after the Bank’s initial implementation of EP—observed continued issues with EP’s 20-point threshold. The 2022 validation report found that “the SAR Yield difference is not statistically significant between uncased event groups with risk score 15 – 19 and cases,” and to address these concerns, “the appropriateness of the current case creation score threshold (20) needs to be justified.”

Instead of adjusting the 20-point threshold in response to the various test reports, Bank of America made other adjustments. In 2022, the Bank responded to a testing finding request to “provide further justification for the modelling choice” used in evaluating EP by testing the 20-point threshold versus an “unconstrained” threshold.<sup>27</sup> Despite finding that the alternative approach of using an “unconstrained threshold” and making corresponding changes to the EP threshold would “uncover more SARs (85.4% vs. 20.2% on below-the-line samples),” the Bank rejected this approach because of the “practical concern of pushing too many below-the-line event groups to cases,” noting that “[g]iven the enormous below-the-line population...the low SAR

---

<sup>27</sup> The “modelling choice” being referenced was a specific value within the “logistic regression model” used in connection with the Bank’s assessment of EP’s performance. In simple terms, the model sought to estimate the probability of an Event Group resulting in a SAR based on the total risk factor weights associated with that Event Group. The specific “choice” that was the subject of this finding was a component of the model (the “intercept”) that represented the probability of an Event Group resulting in a SAR while holding equal all other values of the model. The finding noted that although using the value of “-20” that the Bank selected for this aspect of the model “may seem to be in line with the predefined 20-point creation threshold, however, our independent testing reveals that the alternative model specification where the intercept is estimated by the model *outperforms the [existing] model in all performance measures; it also largely improves the detection of below-the-line SARs*, whereas the [existing] model has very limited effect on reducing below 20 points risk.”

Yield *may exhaust the investigation resources* and prevent from directing the most urgent cases for immediate action.” However, the expected relatively low SAR yield was roughly three to five times the eventual benchmark the Bank later adopted. As indicated above, the response to this testing also failed to address the increasing SAR yield for Event Groups with scores of 16-19 (*i.e.*, just below the 20-point threshold), which had generally exceeded the SAR yields recently observed by the Bank for Event Groups deemed to warrant investigation.

Similarly, in 2023, Bank of America’s former Global Head of Financial Crimes directed a senior manager to repeat a test of EP evaluating SAR yields of cases below EP’s 20-point threshold, with the repeated test assessing as “incorrect” the prior test’s finding of an 18% SAR yield; this SAR yield was used to determine whether “case outcomes [were] reflective of expectations of the [BSA Officer] and [were] suitable for tuning. . . automated detection.” The report of the second test supported the 20-point threshold and pointed to investigator inexperience and biased sample selection for “incorrect” and “unreliable” findings in the previous test. The second test concluded that the team was “confident that EP is working as intended.”

**d) EP “Rescored” or “Suppressed” Alerts Without Adequate Testing and Materially Relied on Auto-Promotions**

EP automatically “rescored” some risk factors to zero, preventing these risk factors from contributing to an Event Group’s overall point value for case generation, which would lead to delays in identifying suspicious activity. However, these “rescoring risk factors” were developed in an “*ad-hoc and subjective fashion.*” In connection with this process, Bank of America developed suppression lists because “[e]vents generated on these entities would be considered false positives which would create noise within investigation cases as they would have been generated by detection channels based on normal business activity and would not represent potential suspicious activity.” Bank of America failed to perform adequate testing during the

Relevant Time Period, to ensure rescoring rules were appropriate and not excluding reportable suspicious activity. Bank of America eventually discontinued the use of such logic in December 2023. At the time, *approximately 150,000 Event Groups* active in EP had triggered one or more aspects of the rescoring logic, “thereby affecting the ability of the [Event Group] to promote to a case.”

One suppression list contained publicly traded companies listed on a group of stock exchanges that were purportedly approved by Bank of America compliance personnel because these publicly traded companies “are considered to have a low money laundering risk.” Despite internal Bank documentation referencing a list of stock exchanges being approved by the Bank’s compliance personnel, Bank of America’s records do not reflect the maintenance of any such list in connection with the relevant rescoring rule within EP.

EP also rescored transactions involving certain cash scenarios for parties on the Bank’s Currency Transaction Report (CTR) Exemptions list, which included businesses for which the Bank believed large currency transactions were routine.<sup>28</sup> The Bank rescored alerts from its cash structuring and ATM payment activity models for potential structuring for customers on this list. The Bank’s documentation acknowledged that FinCEN’s regulation allows banks to exempt certain types of customers with routine needs for large amounts of currency from currency transaction reporting (*i.e.*, filing CTRs).

However, FinCEN’s regulation also provides that nothing in the exemption “relieves a bank of the obligation, or reduces in any way such bank's obligation, to file a [SAR] with respect to any

---

<sup>28</sup> 31 C.F.R 1020.315 eliminates the CTR filing requirement for banks on currency transactions made by certain exempt persons. However, 31 C.F.R § 1020.315(h) expressly provides that “[n]othing in this section relieves a bank of the obligation, or reduces in any way such bank's obligation, to file a [SAR] with respect to any transaction, including any transaction in currency that a bank knows, suspects, or has reason to suspect is a transaction or attempted transaction that is described in § 1020.320(a)(2)(i), (ii), or (iii).”

transaction.”<sup>29</sup> From 2018 to 2024, Customer B (described in the CDD section below) had more than 20 Event Groups indicative of potential money laundering in EP that contained one or more alerts for “Structured cash deposit transactions from business parties” that were all rescored to zero due to the large cash reporting exemption. Of these event groups, only three ever reached the 20-point threshold to become a case. The rescoring contributed to lower point totals for the relevant Event Groups, which impacted whether and when these Event Groups were investigated.

The Bank’s tests of EP did not include specific coverage of these rescoring rules. A 2022 Model Validation Report identified several risk factors that were rescored, and given a weight of zero, that had high SAR yields, such as a risk factor for “Cash Structuring,” which had a SAR yield of 37%; “large cash deposit – multiple location,” which had a SAR yield of 58%; and “base risk factor for prepaid cash high ATM cash withdrawal amount within 7 days,” which had a SAR yield of 53%. Even after this Model Validation Report identified these rescoring risk factors with elevated SAR yields, Bank of America only removed all rescoring logic in December 2023 after regulatory engagement.

EP had certain risk factors that would auto promote Event Groups to become cases immediately, as the “promote risk factors” were weighted with 20 points to meet the case creation threshold. Similar to alerts that were rescored to zero, promote risk factors were also developed in an “ad-hoc and subjective fashion.” A material portion of these promote risk factors were based on seizure warrants, grand jury subpoenas, or employee referrals. For several years within the Relevant Time Period, more than one-third of the cases created by Event Groups were due to promote risk factors, with this number peaking at nearly 50% in 2023.

---

<sup>29</sup> 31 C.F.R. § 1020.315(h); *see also* FinCEN, [FinCEN Advisory, Issue 10: Reformed CTR Exemption Process: Questions & Answers](#) (Oct. 1998), (“This rule does not exempt financial institutions from reporting suspicious activity involving these exempted entities.”).

This high percentage of cases created by promote risk factors demonstrated a material reliance on promote risk factors stemming from external events, like subpoenas or manual referrals, rather than focusing on whether existing risk factors within EP were appropriately tuned to capture suspicious activity. For example, FinCEN’s analysis found that ***80% of the AML investigative cases involving Customer B between 2018 and 2023 included at least one employee referral or external event (law enforcement outreach or 314(b) requests) within the Event Group***, thus indicating that most investigations for this high-risk corporate customer did not result from simple point accumulation based on risk factors reaching the 20-point threshold.<sup>30</sup>

**e) Failure to Effectively Monitor Negotiable Instruments and Credit Cards as well as to Maintain Scenarios to Detect TBML**

For the duration of the Relevant Time Period, EP included only limited coverage of negotiable instrument deposits. Although the Bank maintained a model covering negotiable instruments, it applied to only certain purchases of negotiable instruments and ***did not include any coverage of deposits***.<sup>31</sup> One of the causes of this substantial gap was that Bank of America’s systems did not distinguish between types of negotiable instruments, such as checks or money orders, impeding the Bank’s ability to conduct more targeted, product-specific monitoring.

With respect to the examples described in Section II.D.3, *infra*, these automated monitoring gaps were further exacerbated by Bank of America’s failure to consider negotiable instruments as part of periodic activity reviews that the Bank performed as part of its CDD processes for certain high-risk customers. Notably, FinCEN’s investigation found that, from October 2020 to May

---

<sup>30</sup> This analysis covered a Customer B entity whose account activity was associated with a material portion of the customer’s overall activity through the Bank.

<sup>31</sup> The Federal Financial Institutions Examination Council (FFIEC) guidance states: “Criminals have been known to purchase monetary instruments with currency in smaller increments in order to avoid providing identification or to circumvent BSA requirements, such as Currency Transaction Report (CTR) filings.” FFIEC, [Purchase and Sale of Certain Monetary Instruments Recordkeeping](#).

2025, two online auto auction corporate customers at Bank of America processed tens of billions of dollars in negotiable instrument deposits that had been purchased at third-party financial institutions, which deposits the Bank were effectively not monitoring and resulted in Bank of America failing to report suspicious money order deposits totaling over \$600 million. These suspicious transactions were tied to, among other priority illicit finance risks, activity indicative of potential TBML with a nexus to the southwest border and fraud.<sup>32</sup> Bank of America staff were aware that these customers were tied to high-risk activity. Another financial institution flagged the exact pattern of activity of concern (*i.e.*, potentially structured purchases of negotiable instruments from the requesting financial institution), but Bank of America failed to appropriately monitor or report such activity. As of 2025, a third-party consultant found that despite revising its negotiable instrument policies and resolving rescoring issues in EP, Bank of America still had not conducted a coverage assessment for negotiable instrument products.

Although the Bank's failure to adequately monitor and report suspicious money order deposits was concentrated in these online auto auction customers, it extended to unrelated entities and individual customers in other industries. Another customer in the precious metals industry received, over an approximately three-year period, over 3,500 deposits of negotiable instruments that were purchased at other financial institutions in round-dollar amounts totaling nearly \$3 million. As EP included only limited coverage of negotiable instrument deposits, EP did not alert on these suspicious negotiable instruments. An individual consumer, who claimed to be an investment adviser, deposited millions of dollars across thousands of transactions during a roughly three-year period, including hundreds of thousands of dollars in sequential, round-dollar money orders they purchased at other financial institutions. The relevant activity never generated an alert.

---

<sup>32</sup> See Section II.F.1, *infra*.

Bank of America eventually filed late SARs on this activity, but the Bank instituted a control to identify potentially suspicious activity involving the negotiable instrument deposits by customers only after FinCEN, through its investigation, specifically identified the broad-based nature of the concerns regarding the Bank's controls applicable to negotiable instruments.

Bank of America's credit card monitoring for certain types of activity also was insufficient and resulted in failures to detect and report material suspicious activity tied to an emerging typology of concern, as detailed in Section II.F.3, *infra*. FinCEN's investigation identified that the Bank filed late SARs on hundreds of millions of dollars in transactions indicative of CMLNs involving potential TBML,<sup>33</sup> which was tied to, among other activity, high volumes of back-to-back credit card purchases. As described in more detail in Section II.F.3, *infra*, some of these transactions were processed after the Bank made certain enhancements to EP's threshold. Bank of America also had other internal control<sup>34</sup> and data quality issues with its credit card products, including deficiencies in triggering investigations when a credit card holder's spending routinely exceeded stated income and incorporating credit card activity into the Bank's customer risk assessment process.

A regulatory examination found that, although in January 2024, Bank of America had developed a "TBML Feature" to serve as an indicator of potential TBML activity, including involving credit card activity, the Bank was using this "Feature" only in connection with activity

---

<sup>33</sup> FinCEN issued an advisory on August 28, 2025, which included two red flag indicators for credit card usage tied to CMLNs: 1) "A business that sells electronics or other luxury goods makes payments for multiple credit cards associated with various individuals, who are seemingly unrelated to the business" and 2) "A customer, especially a Chinese national, regularly uses a credit card to purchase large volumes of electronics or other luxury goods." FinCEN, FIN-2025-A003, [FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds](#) (Aug. 28, 2025).

<sup>34</sup> Bank of America did not have limits regarding the number of additional credit cards that can be authorized on the same account. For consumers, there was no limit to the total number of credit cards that can be authorized, but there were limits to the number of users on each card. However, for small businesses, there was no limit to the number of additional cards and authorized users that could be added to credit cards.

that was already the subject of an investigation; Bank of America did not deploy this “Feature” during the Relevant Time Period to generate alerts or trigger investigations to proactively monitor for potential TBML.

These regulatory examination findings underscored similar findings in a 2025 third-party review of EP, which had determined that risk factor weights remained improperly calibrated and that the Bank “does not maintain sufficient detective monitoring capabilities for suspicious activity related to the Trade-Based Money Laundering Red Flag Theme.” The third-party review also found monitoring gaps for credit cards in EP’s “Cash Structuring” model until the model was redeveloped in October 2024, after which credit card activity made up approximately 10% of the transactions monitored by this model. The third party further recommended a lookback to detect suspicious activity related to credit card products.

## 2. Independent Testing

Bank of America’s independent testing function failed to properly detect and describe issues associated with the effectiveness of EP, which as explained above, represented the Bank’s primary internal control to comply with the obligation to identify and report suspicious activity. As detailed in the preceding section, although the underlying data demonstrated that core aspects of EP’s design and implementation resulted in the Bank failing to timely report suspicious activity, internal reports summarizing tests of EP failed to meaningfully address such apparent issues,<sup>35</sup> or

---

<sup>35</sup> Despite multiple testing reports demonstrating that risk factor weights were improperly calibrated relative to their high SAR yields, the Bank failed to meaningfully increase such weights. Although certain of these reports did highlight this disconnect, others did not do so. For example, the April 2020 report revealed a critical gap in the Bank’s alert model testing. Despite finding that certain cash structuring alerts with low risk factor weights (1-2 points) produced high SAR yields, the report recommended **lowering** the weight for a single type of alert with a comparatively low SAR yield rather than **raising** weights for the several other alerts with high SAR yields. Similarly, the Bank’s testing of the 20-point threshold for an Event Group to warrant an investigation did not provide an objective evaluation of EP’s effectiveness in timely identifying and reporting suspicious activity: as explained above, the SAR yields for Event Groups below the 20-point threshold increased over time such that they eventually exceeded the SAR yields for Event Groups above the threshold that the Bank had previously identified as warranting investigation.

if they did include a discussion of the issue, the actions that the Bank purported to take in response did not meaningfully change the relevant aspects of EP.<sup>36</sup>

### **3. Customer Due Diligence Deficiencies**

As part of its obligation to implement and maintain an effective AML program, Bank of America was required to maintain risk-based procedures to conduct ongoing CDD. As described below, Bank of America willfully failed to implement processes that fulfilled this aspect of its AML Program.

To comply with this regulatory requirement, a financial institution's CDD processes must, among other things, allow it to: (i) understand the nature and purpose of the customer relationship for the purpose of developing a customer risk profile, (ii) conduct ongoing monitoring of the accounts to identify and report suspicious transactions, and (iii) on a risk basis, maintain and update customer information (including beneficial ownership information of legal entity customers).<sup>37</sup> As described below, Bank of America's CDD processes failed to accomplish these objectives.

***Overview of the Bank's Failure to Understand the Nature and Purpose of Customer Relationships.*** As detailed below, Bank of America failed to develop customer risk profiles that adequately reflected the nature and purpose of its relationships with certain higher risk customers. In particular, and as highlighted in the examples set forth below, the Bank did not incorporate into customer risk profiles several material risks that arose from these customers through the Relevant Time Period, including instances in which Bank personnel raised concerns. These risks included the relevant corporate customers' heavy reliance on third-party payments (*i.e.*, payments from

---

<sup>36</sup> Rather than reasonably responding (*i.e.*, by changing the threshold), the Bank sought to continue to justify the existing threshold, including by citing to the impact that would have on Bank resources and, in one instance, re-performing the test, the result of which purported to produce a result that supported maintenance of the same 20-point threshold.

<sup>37</sup> 31 C.F.R. § 1020.210(a)(2)(v).

persons with whom the Bank's customer had no direct relationship). Bank personnel acknowledged that such payments, among other things, limited the Bank's visibility into the true source of funds entering the customers' accounts and complicated Bank of America's ability to determine whether the transactions were consistent with the customers' expected activity—factors that FinCEN has identified as potentially relevant for customer due diligence purposes.<sup>38</sup> The Bank also did not adequately consider the customers' international business activities, geographic footprints, and exposure to high-risk jurisdictions—including indirect exposure through affiliated entities—with elevated TBML and sanctions evasion risks.<sup>39</sup>

One of the Bank's mechanisms for assessing customer risk during the Relevant Time Period was its "Dynamic Risk Rating" process, which was designed to assign and periodically update customer risk ratings based on customer characteristics, products and services utilized, geographic exposure, and other risk factors as they arose. Those risk ratings, in turn, were intended to inform the level of customer due diligence, periodic review, and ongoing monitoring performed for such customers. As discussed below, however, this process, as applied, was flawed in both design and implementation, with the risk rating being informed by the Bank's receipt of law enforcement subpoenas and not reflecting, for example, that the relevant customers had triggered an "*insane*"

---

<sup>38</sup> See, e.g., FINCEN, [\*Frequently Asked Questions Regarding Customer Due Diligence \(CDD\) Requirements for Covered Financial Institutions\*](#), FIN-2020-G002 (Aug. 3, 2020), (heightened risk can be mitigated by, among other things, enhanced monitoring and collecting information regarding expected account activity); see also FFIEC, [\*BSA/AML Manual, Customer Due Diligence- Overview\*](#) (listing additional information that can be collected as part of EDD); FINCEN, [\*Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions\*](#), FIN-2018-G001, Qs. 35-37 (Apr. 3, 2018) (explaining that information concerning the nature and purpose of a customer relationship should establish a baseline against which expected activity – including expected use of wires and typical deposit activity – can be assessed, and that changes in activity may warrant updates to customer information through risk-based monitoring); FINCEN, [\*Guidance on Obtaining and Retaining Beneficial Ownership Information\*](#), FIN-2010-G0001 (Mar. 5, 2010), (for heightened-risk accounts, enhanced due diligence may include steps to understand the sources and uses of funds; CDD/EDD information should be used for monitoring to identify discrepancies between the account's intended purpose and expected activity and the actual sources and uses of funds).

<sup>39</sup> During the Relevant Time Period, one customer's dynamic risk rating changed several times between "standard," "elevated," and "high," with significant risk rating changes appearing to directly correlate with the Bank receiving subpoenas or other law enforcement inquiries rather than the Bank's own risk assessment processes.

amount of investigations for potentially suspicious activity. Similarly, although the Dynamic Risk Rating model was designed to incorporate negative news, it failed to incorporate one customer's public disclosure in a securities filing that it was under investigation by the Department of Justice for potential violations of money laundering laws.

***Overview of the Bank's Failure to Conduct Adequate Ongoing Monitoring.*** As further detailed below, certain of the Bank's ongoing monitoring processes, which should have been reasonably designed to identify and report suspicious activity, were deficient and did not timely identify suspicious activity associated with these customers. The Bank also failed to adequately maintain and update customer information on a risk basis, including by failing to sufficiently incorporate material information into these customers' risk profiles and ongoing monitoring. Although at times the Bank's Dynamic Risk Rating scores identified the relevant customers as presenting elevated or high financial crime risk, the Bank's ongoing monitoring was not responsive to such risks. For example, the Bank conducted quarterly "Client Activity Monitoring" reviews for customers designated as elevated or high risk. These reviews were designed to supplement automated monitoring by assessing whether a customer's activity remained consistent with their expected activity, and whether changes in customer behavior warranted updates to the customer's risk profile, enhanced due diligence, or other monitoring measures.

However, in some instances, Bank personnel repeated observations from one quarter to another, and the relevant observations failed to take into account information about the customer's activities relevant to assessing the risks posed by these customers, such as the total value of the customer's activity in the relevant quarter or the jurisdictions associated with the customers' transactions (even when, for example, the Bank's automated monitoring system had already generated numerous alerts for such customer's transactions involving high-risk jurisdictions).

These quarterly reviews did not address the negotiable instruments that these customers received and deposited into their Bank of America accounts, with these quarterly reviews omitting any analysis of such activity even where there were tens of billions of dollars in such instruments being deposited. This gap persisted even after the Bank became aware that the negotiable instruments deposited by one of these customers appeared to reflect structured activity designed to evade a BSA obligation. The Bank likewise failed to timely identify and respond to material deviations between customers' expected activity and their actual transactional activity, including for one customer onboarded as a "small-medium" commercial customer with expected annual sales of \$1 to \$4 million yet which received wires from high-risk jurisdictions amounting to multiple orders of magnitude greater than this expected level of activity. The Bank similarly did not timely identify and assess geographic activity that was inconsistent with the customers' expected business operations—including substantial volumes of activity involving high-risk jurisdictions—with the Bank's limited scope periodic reviews failing to capture any information about geographic trends involving the customers' activities.

**a) Overview of Customer A, Customer B, and Customer C**

Customer A is a company that operates a global, digital marketplace connecting sellers of salvaged vehicles sourced in the United States with both domestic and international buyers. Bank of America maintained accounts for Customer A dating back to 1995. During the Relevant Time Period, the business relationship generated annualized revenue of several million dollars a year. Bank of America also served as lead agent in a refinancing of \$200 million that formed part of a broader credit facility worth over \$1 billion.

Customer B is a publicly traded company that similarly operates a platform linking sellers of U.S. salvaged vehicles with buyers around the world. The Bank has maintained accounts for

Customer B since 1996. During the Relevant Time Period, the Bank’s total revenue from Customer B exceeded \$25 million. In recent decades, Customer B experienced a substantial increase in the proportion of international buyers of vehicles on its platform.

Customer C is a vehicle export business that maintained commercial relationships with both Customers A and B. Although the Bank classified Customer C as a “small-medium” business with expected annual sales of \$1 to \$4 million—as detailed below, during the Relevant Time Period, Customer C received hundreds of millions of dollars in cross-border wires from Eastern Europe (principally, Georgia)—the volume of such activity substantially exceeded this customer’s expected activity as reflected in the Bank’s CDD materials, which also failed to identify Customer C’s commercial relationships with entities operating in multiple high-risk jurisdictions. Although activity involving Eastern Europe could have been viewed as generally consistent with the geographic footprint of Customer C’s business, the volume of activity substantially exceeded the expected activity for Customer C. Customer C’s accounts at the Bank were closed in January 2024 after the Bank filed multiple SARs identifying Customer C as a subject, but the Bank did not correspondingly reassess or enhance its due diligence procedures for Customers A or B, which continued to transact and maintain publicly disclosed commercial relationships with Customer C.

The potential money laundering risks that could be associated with vehicle auction and export businesses have long been recognized by FinCEN and other law enforcement agencies.<sup>40</sup>

---

<sup>40</sup> See U.S. DEPARTMENT OF THE TREASURY, [2018 National Money Laundering Risk Assessment](#) (Dec. 2018); U.S. DEPARTMENT OF THE TREASURY, [2024 National Money Laundering Risk Assessment](#) (Feb. 2024) at 48 (noting that criminals often use illicit cash to purchase bulk money orders and then use the money orders to “purchase material assets, such as cars, and export the vehicles or assets to a foreign country.”); see also FINCEN, [Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Trade-Based Money Laundering](#), FIN-2010-A001 (Feb. 18, 2010) (identifying third-party payments and negotiable instruments, including cashier’s checks and money orders, as potential indicators of TBML, including where such instruments are used to pay for goods and services); DEPARTMENT OF JUSTICE, [Tampa Man Pleads Guilty to Money Laundering](#) (Feb. 1, 2016) (defendant pleaded guilty to money laundering after admitting that he planned to use purported heroin proceeds to purchase vehicles for export to Lebanon and resale overseas).

Used vehicle transactions have repeatedly been publicly linked to TBML and terrorist financing networks, as used and salvaged vehicles can be used to move value across borders.<sup>41</sup> The Bank's investigators were aware that used vehicle exports could be a component of money laundering schemes.

The Bank should have been especially vigilant about these specific customers because, as detailed below, the business models of both Customers A and B relied heavily on payments received from third parties, including international buyers and through non-transparent means, such as money orders from unknown purchasers—a practice that Bank compliance personnel identified as one of the bases for a recommendation to offboard Customer A, which recommendation the Bank did not ultimately accept during the Relevant Time Period.<sup>42</sup> Additionally, in November 2023, one of these customers publicly disclosed that the Department of Justice was conducting an ongoing investigation into potential violations of money laundering laws relating to its anti-money laundering practices.

Although the Bank filed SARs involving Customers A and B during the Relevant Time Period, most of those filings did not address money order deposits into the customers' accounts at the Bank or the underlying vehicle buyers associated with those transactions. Moreover, the information developed through the Bank's suspicious activity reporting generally did not result in meaningful reassessments of the risks presented by these customer relationships or corresponding

---

<sup>41</sup> See FINCEN, *Finding That the Lebanese Canadian Bank SAL Is a Financial Institution of Primary Money Laundering Concern*, 76 Fed. Reg. 9403 (Feb. 17, 2011) (identifying used vehicle exports as a TBML typology employed to move illicit proceeds internationally, including through a network that benefited Hezbollah).

<sup>42</sup> Although Bank compliance personnel initially recommended terminating the relationship with Customer A, FinCEN does not suggest that account closure is the only appropriate response to heightened financial crime risk. Rather, once a bank identifies elevated risks associated with a customer relationship, it must implement customer due diligence, ongoing monitoring, and other controls reasonably designed to mitigate those risks. Although account closure may be appropriate in certain circumstances, banks may also mitigate identified risks through enhanced monitoring, restrictions on products or services, or other risk-based controls.

changes to the Bank's due diligence, ongoing monitoring, or other risk-mitigation measures. These deficiencies were particularly significant given the substantial volume of third-party payments received by Customers A and B, including billions of dollars in cross-border wires and tens of billions of dollars in negotiable instruments.

**b) Bank Knowledge of Customer Risks and Lack of Meaningful Response**

***Events Prior to 2019 Established the Nature and Extent of the Risks Posed by Customers***

***A and B.*** As early as 2016, Bank personnel identified significant risks associated with Customer A's business model, including the receipt of international wire transfers from high-risk jurisdictions, limited transparency regarding the identities of underlying buyers of vehicles being sold on Customer A's platform, and insufficient visibility into the source of funds supporting vehicle purchases. Case notes in March and July 2016 also show transactions that were related to investigations into ***narcotics trafficking through the purchase and shipment of vehicles***. In connection with these 2016 investigations of Customer A, Bank compliance personnel indicated that Customer A had previously been contacted after compliance personnel raised concerns related to wire transfers originating from high-risk jurisdictions, noting that Customer A had purportedly agreed to undertake "an in-depth look at their overall KYC process and transaction review."

***Events from 2019 to Mid-2022 Amplified the Nature and Extent of the Risks Involving***

***Customers A and B.*** Beginning in 2019, the Bank's monitoring and investigative processes repeatedly identified potentially suspicious activity involving Customers A and B that presented indicators of elevated money laundering risk, including cash structuring, wires involving high-risk jurisdictions, unusual transaction volumes, and other potential money laundering indicators identified by EP in connection with Customer B.

By early 2020, the Bank had accumulated several years of internal investigations, transaction monitoring alerts, and law enforcement inquiries involving Customer B. Nevertheless, Customer B's Dynamic Risk Rating remained "Standard" until the Bank received a grand jury subpoena in February 2020. Shortly thereafter, the Bank increased Customer B's Dynamic Risk Rating first to "Elevated" and then to "High," with no meaningful impact to enhanced customer due diligence or modifications to the Bank's ongoing monitoring of Customer B's activity. In March 2020, a Bank investigator documented discussions with law enforcement regarding concerns that Customer B's accounts may have been connected to a money laundering scheme involving another Bank customer through the use of cashier's checks.

During the same period, compliance personnel also analyzed activity involving Customer A and, in April 2020, identified Customer A's accounts as having been used by a fraud ring involving stolen checks. Between June and July 2020, the Bank documented multiple investigations involving Customer A's accounts that were associated with *business email compromise scams, elder fraud, and other fraud schemes*. Internal case notes repeatedly reflected that, although Customer A was considered a suspect or otherwise was associated with suspicious activity, its customer relationship would remain open. For example, in case notes of a June 2020 investigation, Bank personnel noted that "*although [Customer A] is considered a suspect, account will not be closed. Issue has been escalated to the client team on multiple occasions; however, closure is not supported.*"

By October 2020, investigators continued to identify Customer A in investigations involving multiple fraud typologies. Internal case notes described Customer A's account as being involved in "*numerous cases with scam activity ([Business Email Compromise], Romance Scam, Nigerian Scam, Covid)*" in which Customer A's account received funds from activity that

the Bank had identified as fraudulent, and that the account would be escalated for further review by the Bank’s AML function. Similar case notes observed that Customer A’s account activity was “so vast” that the Bank’s internal investigative system was unable to download the relevant transactions for review.

By 2021, the Bank’s existing concerns regarding Customers A and B were supplemented by information from other financial institutions raising additional concerns regarding these customers. In September 2021, the Bank received a request for information from a money services business (MSB) regarding possible structured purchases of negotiable instruments issued by the MSB and subsequently deposited into Customer B’s account at the Bank, including activity potentially designed to evade applicable recordkeeping requirements. In responding to the request, the Bank stated that, among other things, it did not see any unusual pattern of velocity followed by the money order deposits, and that there was no transactional activity or behavior to indicate the account may be engaging in or abetting illicit activity. The Bank did not revise Customer B’s risk profile, perform additional due diligence, or modify its ongoing monitoring, which continued to omit altogether Customer B’s high volume of negotiable instrument deposits.

Beginning in late 2021 and into mid-2022, Customer A also experienced significant increases in international wire activity, including increased transaction volume ***upwards of \$1.7 billion dollars*** involving jurisdictions bordering Russia contemporaneous with the Russian invasion of Ukraine. These changes in activity indicated a potential material shift in the geographic risk presented by Customer A, including because of the contemporaneous increased regulatory and law enforcement attention to the risks of intermediary jurisdictions—such as Belarus and Georgia—as potentially facilitating sanctions evasion and TBML.<sup>43</sup>

---

<sup>43</sup> See FINCEN, [\*FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts\*](#), FIN-2022-Alert001 (Mar. 7, 2022); see also FINCEN & BIS, [\*FinCEN and the U.S. Department of Commerce’s Bureau of Industry\*](#)

Such transactions with a nexus to these jurisdictions later became the subject of external requests, including a July 2022 request for information that Bank of America received from another financial institution regarding certain of Customer A's transactions with a nexus to Georgia, as well as similar transactions that the Bank processed for Customer C. Subsequent internal Bank of America analyses focused on the significant volumes of incoming wire transfers from Belarus and concluded that portions of the activity appeared to be outside of Customer A's documented geographic footprint. The Bank did not file a SAR reporting this activity until August 2023, and did not report the bulk of the activity until June 2025. The activity reported in June 2025 included certain wire transfers involving Customer C that another financial institution had previously identified in its July 2022 request for information to the Bank. Despite these developments, the Bank did not update Customer A's risk profile or conduct enhanced monitoring to account for this change in Customer A's activity.

***Events from Mid-2022 to Mid-2023 Reflect Escalation by Bank Compliance Personnel of Risks Involving Customers A and B Without Corresponding Mitigation Measures.*** In May 2022, Bank compliance personnel investigated reports that a website directing individuals to purchase convertible virtual currency instructed purchasers to wire funds into one of Customer A's accounts at the Bank, thereby indicating that Customer A's account may have been used to move the proceeds of an investment scam involving convertible virtual currency.<sup>44</sup> Upon further review, Bank compliance personnel recommended that Customer A be presented to a Bank committee associated with closing customer accounts because the customer appeared to be operating in a

---

[and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts](#), FIN-2022-Alert003 (June 28, 2022).

<sup>44</sup> The Bank subsequently determined that Customer A's account had been compromised and that Customer A was not knowingly participating in the suspected scam.

manner inconsistent with its understood business model. As the investigation into this apparent fraud scheme progressed, however, compliance personnel identified broader concerns extending beyond the initial convertible virtual currency issue. Internal communications reflected compliance personnel concerns regarding Customer A's acceptance of third-party payments, limited visibility of the source of funds moving into Customer A's accounts, the volume of AML investigations involving Customer A, and the possibility that the accounts were facilitating broader financial crime. In July 2022, compliance personnel recommended that Customer A's accounts be considered for closure due to these risks.

Following a review of Customer A's account the Bank's internal analysis demonstrated that the company had become the subject of numerous Bank compliance investigations, with this employee noting that *Customer A had been associated with over 100 cases from 2020 to August 2022*, with the majority of them representing “*fraud cases due to incoming payments via wires [and] checks*,” prompting a fellow compliance employee to reply “*YESSSSSSSSSSSSSS . . . Concern that the client does not have visibility or understanding of source of funds*,” and, on a related email thread, another compliance employee to respond to the case volumes and inquiries from law enforcement related to Customer A with “*WOW*.” Internal communications noted repeated research requests from a law enforcement agency involving fraudulent wire transfers directed to “[Customer A] Buyer” accounts and described recurring links between activity in Customer A's account and business email compromise schemes, romance scams, advance-fee fraud, fraudulent checks, and virtual-currency related activity. The same communications also referenced related *law enforcement interest in Customer A's account activity from at least five different Federal agencies*.

Bank compliance personnel concluded that the central concern with Customer A's accounts was not limited to any single fraud typology, but rather that "the client does not have visibility or understanding of source of funds," with a compliance employee stating that there was "*to[o] much risk and no evident way to control/mitigate it[.]*" In an August 2022 meeting with the business team managing the Customer A relationship, Bank compliance personnel stated that, between 2020 and August 15, 2022, more than 100 AML cases had been identified involving Customer A, approximately 90% of which were fraud-related, and that "*[o]verwhelming evidence suggests that [Customer A] is receiving payments from numerous victims of mass marketing scams[.]*" Contemporaneous communications among Bank compliance personnel showed that they "expect[ed] some pushback on the closure" because Customer A was a "longstanding client and there is significant credit exposure."

After the Bank's relationship team held additional discussions with Customer A in September 2022, compliance personnel continued to assess the risks presented by the relationship and began evaluating whether those risks extended to other online auto auction customers. As part of this review, Bank compliance personnel compared investigative metrics and case volumes across the Bank's online auto auction relationships, with compliance personnel concluding that Customer B raised "similar concerns," but exhibited these concerns "in significantly lower scale/volume" than Customer A. Based on this preliminary analysis, compliance personnel indicated that they would "pursue an analysis of all Auto Auction companies in the future to understand the risk associated with these types of companies." The Bank did not conduct such an analysis for another two years, eventually conducting it only after FinCEN's investigation was well underway.

Following a September 2022 internal meeting, Customer A's relationship manager prepared a memo responding to the concerns compliance personnel had raised regarding Customer A's accounts over the preceding months. This memo described Customer A as "a large and valued client" generating approximately \$6 million in annual revenue, the Bank's broader lending and treasury management relationship with Customer A and its affiliated entities, and the relevant line of business being "**very supportive** of our important relationship with [Customer A]."45

Compliance personnel responded with questions related to the risks Customer A posed and how such risks were being mitigated, including whether Customer A accepted payments from third parties and whether any controls applied to those payments. The responses compliance personnel received confirmed that Customer A accepted payments directly from people other than the registered buyer and also noted that Customer A generally subjected international buyers to the same registration process as domestic buyers. Compliance personnel continued to express significant concerns regarding the relationship, including by describing "*an insane amount of cases/investigations*," that the customer "does not understand source of funds in account," and "money laundering concerns, *potentially facilitating transnational crime*."

In preparation for a November 2022 meeting with a foreign financial institution for which Bank of America maintained a correspondent account, compliance personnel identified significant incoming wire activity associated with the Bank's auto auction customers (including Customer A) involving Belarus and noted that similar activity could exist involving other higher-risk jurisdictions. However, the Bank failed to conduct an adequate analysis until March 2023 and did not file a SAR involving Customer A's relevant activity until February 2025.

---

<sup>45</sup> Emphasis in original.

During the same period, compliance personnel finalized briefing materials regarding the recommended termination of Customer A (which had now been pending for roughly four months) for the Bank's then-BSA Officer, while updating a slide deck that continued to recommend closure of Customer A's accounts. The slide deck reflected that, since 2020, Customer A had generated more than 250 referrals and over 125 AML investigations, approximately 90% of which were fraud related, and significant international transactional activity that "appears to be out of [geographic] footprint," including 290 incoming wires to Customer A's account from Belarus in August 2022 alone that totaled \$3.5 million. The materials further noted that, although there was no evidence that Customer A orchestrated the underlying fraud, "the sheer volume" of referrals and investigations was "notable," the account appeared to have "funneled fraud proceeds," and the closure recommendation for Customer A's accounts remained in effect. Email correspondence showed that, consistent with the prior memo that had been prepared, "the relationship team is very supportive of our important relationship with [Customer A]."

Similarly, notwithstanding Customer B's high-risk designation and the Bank's continued internal discussions regarding third-party payments, international wire activity, and high volumes of negotiable instrument deposits, the Bank's ongoing monitoring of this customer remained largely unchanged. For example, during the fourth quarter of 2022, Customer B received approximately \$1.1 billion in wire transfers from its affiliate in the United Arab Emirates, an increase of more than 200% compared to the same period in 2021. Although Customer B was classified at this time as a high-risk customer, the corresponding quarterly client activity review process neither identified nor discussed this significant increase in international wire activity or its implications for Customer B's risk profile.

In December 2022, compliance personnel directed the financial crimes analytics team to conduct an additional review of publicly available information and other financial crime indicators related to Customer A. Although investigators did not identify evidence that Customer A was involved with fraud schemes, internal communications acknowledged that the online auto auction industry presented inherent fraud risks and recognized that the customer relationship carried significant risks.

In anticipation of a meeting between the BSA Officer at the time and the head of the relevant business line to discuss Customer A, the BSA Officer requested updated information regarding Customer A. In response, compliance personnel confirmed that their recommendation to close Customer A's accounts remained in effect. Following the late December 2022 meeting between the BSA Officer at the time and the head of the relevant line of business, the relationship team continued to advocate for maintaining the business relationship, noted Customer A's commercial importance, and proposed customer-specific mitigation measures. In doing so, the relationship manager for Customer A acknowledged that *“the industry isn't the cleanest so there is always fraudster risk here,”* but cited to processes that Customer A represented it had developed that gave the line of business comfort regarding how Customer A transacted through the Bank, adding that *“a closure here would be detrimental given the impact of this relationship.”* Ultimately, a March 2023 mitigation plan was developed that represented an alternative to compliance's recommendation to close Customer A's accounts.

While the line of business continued to develop arguments to maintain Customer A's accounts, compliance personnel documented conversations with a member of U.S. law enforcement, with compliance personnel noting in January 2023 that a *“law enforcement investigation considers the activity through these [online auto auction] companies to be money*

*laundering.*” The following month, compliance personnel noted that U.S. law enforcement indicated that extensive data analysis had identified patterns of repeated vehicle purchases by certain buyers and connections among purchasers, suggesting related activity rather than isolated transactions.

In parallel with these discussions with U.S. law enforcement, compliance personnel continued following up with the business relationship manager about “further developments on proposed next steps to reduce/mitigate risks with [Customer A] exposure.” Compliance personnel “stress[ed] that the main concern[] is external third party fraud risk . . . this means *we are most concerned about the risk that fraudsters are using [Customer A’s] accounts to mislead, intimidate or obfuscate funds from victims to be used by fraudsters for illicit purposes*” and also provided the business with additional examples supporting this concern, including “*receiving proceeds from prepaid unemployment fraud,*” and eight examples of incidents that took place between the months of September and October 2021 alone of *Customer A having received “proceeds from various scams.”* After employees in the relevant line of business indicated that additional time was required, compliance personnel cautioned that “*swift action to reduce this kind of activity is key,*” as “*otherwise, closure will be the only option.*”

In March of 2023—*more than six months after compliance personnel recommended that Customer A’s accounts be closed*—the relationship manager arranged a call with representatives of Customer A and the relevant compliance personnel from Bank of America. In summarizing the discussion with Customer A, the relationship manager listed a series of four mitigation measures: (i) “Require that [Customer A] only accept payments for vehicles from its registered dealers . . . [t]his will eliminate the Bank receiving wires from sanctioned countries (Russia, Belarus, etc.)” . . . (ii) “Recommend that [Customer A] take down their account number from its website” . . .

(iii) “Recommend that [Customer A] use a new account number given that the existing account number has been compromised” ... and (iv) “Recommend a ‘one strike and you’re out’ policy for dealers that send in a request to return funds claiming “fraud” when there is no “fraud.” Contemporaneous internal communications from compliance personnel stated that the recommendation to close Customer A’s account was being “withdraw[n] . . . based on the communication and implementation of the risk mitigation strategies” while also stating that compliance would “monitor the client implementation of these risk mitigation strategies,” with the possibility that compliance may “revisit and reconsider” its withdrawal of the recommendation to close Customer A’s accounts.

***Events from Mid-2023 to Mid-2025 Reflect that Risks Involving Customers A and B Were Persisting without Sufficient Mitigation.*** Although Bank compliance personnel had identified third-party payments as a central driver of the risks associated with the Customer A relationship, the Bank did not contemporaneously enhance its customer risk profile, periodic customer reviews, or transaction monitoring to account for those risks. Moreover, although one of the central recommendations to Customer A in March 2023 was to “accept payments for vehicles only from its registered buyers/dealers” (*i.e.*, to mitigate the identified risk of Customer A’s acceptance of third-party payments), Customer A continued to process third-party payments through its Bank of America account until June of 2025.

Customer A viewed third-party payments as an integral component of its business model and was unwilling or unable to fully eliminate those payments. The Bank was informed that, rather than ceasing to accept third-party payments, Customer A would instead apply certain controls. The Bank did not, however, update Customer A’s customer risk profile, adjust its ongoing monitoring, or implement other CDD measures commensurate with the risks associated with Customer A’s

continued acceptance of third-party payments. Certain of the other recommendations to Customer A were eventually implemented, including the issuance of a new account number to replace the account that had been referenced in the convertible virtual currency scam that Bank investigators had first identified in the summer of 2022.

In the fall of 2023, subsequent internal reviews reflected that Customer A continued to generate investigations (including fraud-related cases). The Bank continued to monitor Customer A's activity and found that *“the same typology of cases are still present,”* and that *“fraudsters were using Customer A's accounts to mislead, intimidate, or obfuscate funds from victims to be used by the fraudsters for illicit purposes.”* Despite Customer A's mitigation measures, since April 2023, there were similar levels of cases being opened involving Customer A, with increased levels of cases observed into May and June. In December 2023—well over a year after Customer A's accounts were initially recommended for closure—options to mitigate fraud were still being discussed, but did not squarely address the third-party payment risk that the Bank had already identified as the central concern involving Customer A's activities. Compliance personnel recognized “this activity [was] disproportionate to other clients” and that the “discussions had been going on since March.”

Compliance personnel also observed that the volume of cases that Customer B was triggering within the Bank represented *“a high volume for any client*—not just those in this industry.” Internal communications reflected that the Bank's principal concern was that bad actors were using Customer B's platform and accounts to facilitate TBML by purchasing vehicles with illicit proceeds—including with money orders that Customer B was depositing into its accounts at Bank of America—and exporting those vehicles internationally. Customer B was rated “Standard” from July 2022 until March 2023, when its risk rating was changed to “Elevated” after the Bank

received a grand jury subpoena. By September 2023, the Bank was aware that Customer B continued to receive significant negotiable instrument deposits associated with the risks they identified.

Additionally, in November 2023, one of these customers publicly disclosed that the Department of Justice was conducting an ongoing investigation into potential violation of money laundering laws related to its anti-money laundering practices; this disclosure did not result in the Bank making any corresponding changes to this customer's risk profile or to modify the Bank's monitoring of the customer's transactions.

In December 2023, the Bank exited Customer C following its investigation into the customer's international wire activity and its ties to Georgia's international used car market. In addition to its publicly disclosed commercial relationship with Customer B, Customer C had been identified internally as a significant source of international wire activity into Customer A's accounts and had been referenced in the July 2022 request for information that the Bank received from another financial institution, as well as in several SAR filings. The Bank did not reassess the risk profiles of Customers A or B based on this information or implement additional due diligence or monitoring designed to address the risks posed by the continuing relationship that Customers A and B had with (the then-former) Customer C.

Throughout 2024, the Bank continued to pursue customer-specific mitigation measures while evaluating the risks associated with both Customers. In March, after concluding that the existing account had been compromised by the virtual currency scam identified in the summer of 2022, the Bank issued a new operating account to Customer A that replaced the compromised account. Internal communications around this time nevertheless reflected that five of the ten AML

cases generated involving Customer A during 2024 continued to concern third-party payment fraud.

By the end of 2024, Customer B had stopped accepting money orders as a form of payment, while Customer A adopted a more incremental approach by first ceasing to accept money orders purchased from a specific MSB but continuing to accept money orders sold by other MSBs. Additionally, at the Bank's request, Customers A and B retained independent consultants to review aspects of their anti-financial crime programs; these reviews were completed in late 2024, however the Bank did not conduct follow up discussions regarding the results until 2025. During this same period, the Bank continued to evaluate concerns associated with international wire activity, third-party payments, and potential sanctions evasion.

***Events from Mid-2025 to End of Relevant Time Period.*** By mid-2025, concerns regarding third-party payments, source-of-funds transparency, negotiable instrument activity, and international wire activity, were not fully resolved. Customer A continued accepting some money orders until approximately July 2025. The continuation of these payment practices occurred notwithstanding years of internal discussions concerning the risks associated with third-party payments and negotiable instrument activity.

In sum, Bank of America failed to comply with its CDD requirements with respect to these customers because it did not adequately implement risk-based procedures adequate to understand the nature and purpose of high-risk customer relationships, conduct effective ongoing monitoring, and, on a risk basis, maintain and update customer information.

### **E. Due Diligence Programs for Correspondent Accounts for Foreign Financial Institutions**

Foreign correspondent accounts are gateways to the U.S. financial system that can present heightened AML/CTF risks depending on the unique facts and circumstances of the account.<sup>46</sup> Bank of America failed to establish a due diligence program that, with respect to correspondent accounts that the Bank maintained for its own foreign branches and affiliates, satisfied regulatory requirements. Until late 2024, the Bank had a policy permitting “[s]implified” due diligence that imposed “reduced requirements” for the correspondent accounts of the Bank’s foreign branches and affiliates.

FinCEN’s investigation of this issue, which focused on twelve of the Bank’s foreign branches and affiliates, found that the Bank’s “simplified” due diligence caused files for the relevant foreign branches and affiliates to (i) lack sufficient information about the anticipated activity in the correspondent account and the account’s purpose; (ii) contain general statements about the nature of the foreign branch or affiliate’s business and markets served, such as “treasury services” or “cash management;” and (iii) have insufficient information about the supervisory regime applicable to the foreign branch or affiliate, such as merely providing the name of the local regulatory body. These due diligence files often consisted of information irrelevant to the Bank’s ability to detect and report, on an ongoing basis, suspicious activity conducted through or involving the correspondent accounts (*e.g.*, graphs depicting the price of the Bank’s parent holding company’s publicly traded stock).

Although the Bank also separately maintained two other categories of due diligence information—foreign branch risk assessments and industry questionnaires—such materials did not

---

<sup>46</sup> See 31 C.F.R. 1010.610.

comply with the applicable regulatory requirements. *First*, the foreign branch risk assessments of the relevant branches and affiliates were generally several years old, framed as documents to be used by the local management of the foreign branches to help manage their applicable risks, and did not explicitly discuss the foreign branches' correspondent accounts—including their expected activity or the purpose in maintaining such accounts. *Second*, the Bank obtained industry questionnaires in a manner that did not fulfill its regulatory obligations. Some questionnaires were completed by the Bank on behalf of *all* its foreign branches and affiliates, and others were completed for specific foreign branches and affiliates shortly before the Bank changed the applicable policy in December 2024.

One of the apparent causes of this issue seems to have been Bank of America's focus on general attributes of its foreign branches and affiliates, including that they were focused on serving "large multinational corporations...large financial institutions, and institutional investors"—as well as the Bank's emphasis on whether its foreign branches and affiliates maintained accounts for non-U.S. banks (as opposed to non-bank financial institutions) and on the transactions its foreign branches and affiliates processed for non-U.S. banks in the local market primarily related to "interbank settlement" transactions and "bank-to-bank bulk flows."

FinCEN's investigation of this issue found that the relevant branches and affiliates maintained accounts for more than 250 non-bank financial institutions, including MSBs or foreign equivalents thereof. The payments associated with these non-bank financial institution customers were inconsistent with "bank-to-bank bulk flows" or "interbank settlements." Although Bank of America screened transactions to and from the Bank, its failure to collect sufficient due diligence information with respect to its foreign branches and affiliates, including the extent to which those branches and affiliates were expected to use their correspondent accounts to process transactions

on behalf of such MSB clients, resulted in the Bank lacking a sufficient understanding of such accounts—including for the purpose of detecting and reporting known or suspected money laundering.

*Finally*, the 2025 third-party review of Bank of America’s AML program identified additional findings regarding the Bank’s ability to detect and report suspicious activity involving its correspondent accounts. The third party’s report found that certain transaction monitoring models that the Bank applied to its correspondent accounts were too narrow, failed to capture key risks, and allowed high-risk relationships to continue unchecked.

#### **F. Violations of the Requirement to Report Suspicious Transactions**

During the Relevant Time Period, Bank of America failed to file timely and accurate SARs on suspicious transactions totaling over \$5 billion dollars, with over \$1 billion of this activity implicating national security-related and other priority illicit finance risks, including suspicious transactions indicative of CMLNs, fraud, and potential TBML with a substantial nexus to the southwest border. These reporting failures prevented law enforcement from timely receiving critical financial intelligence.

FinCEN’s investigation found that Bank of America’s SAR failures generally related to four categories of violations, each of which is described in the sections that follow: (i) large volumes of money order deposits into the accounts of Customers A and B that, as explained below, showed signs of attempts by the purchasers to evade BSA requirements, with FinCEN’s investigation identifying that many of these deposits had a nexus to the southwest border; (ii) wires with a nexus to high-risk countries involving Customers A, B, and C that were inconsistent with the Bank’s risk profiles associated with these customers and demonstrated signs that such transactions lacked a business or apparent lawful purpose; (iii) transactions involving high volume

credit card activity that appeared consistent with CMLNs, some of which Bank of America failed to timely detect and report even after making certain changes to EP; and (iv) other suspicious transactions that Bank of America failed to report on time because of EP's design.

### **1. Negotiable Instrument Deposits for Online Auto Auction Customers**

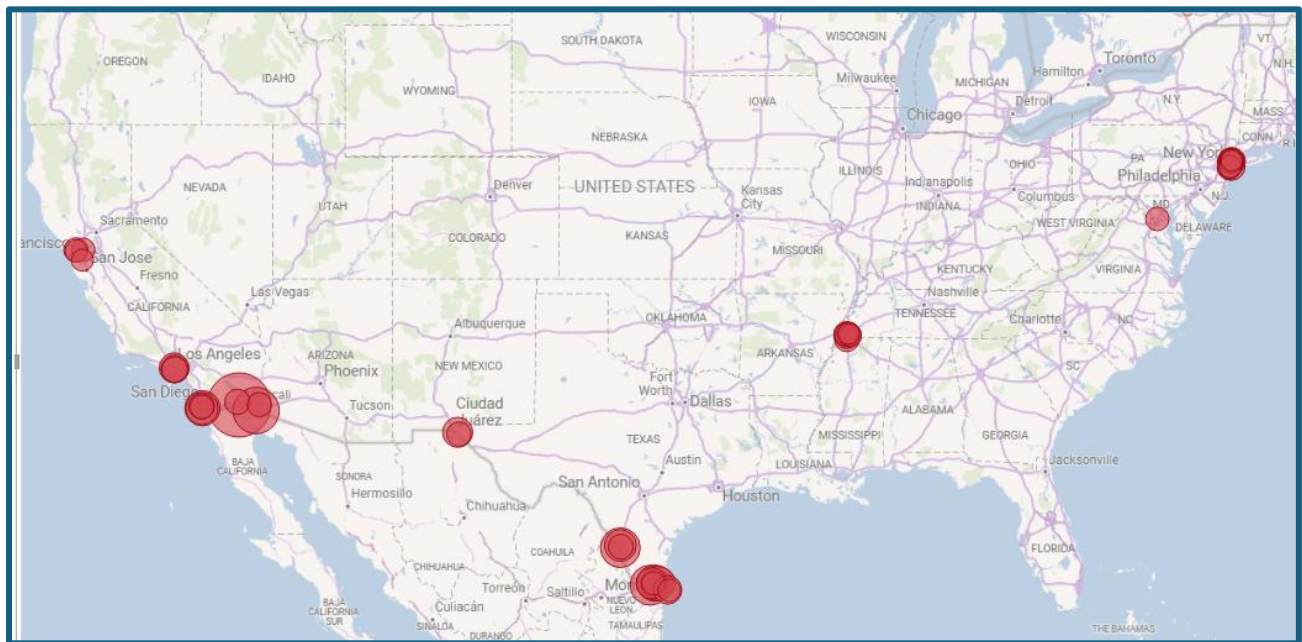
FinCEN's investigation concluded that Bank of America failed to perform adequate monitoring of large volumes of deposits of money orders by Customers A and B,<sup>47</sup> including because: (i) as explained above, EP included only minimal coverage of this type of transactional activity—despite the Bank's online auto auction customers effecting billions of dollars' worth of such deposits; (ii) Bank models did not differentiate between money orders and other types of negotiable instruments, thereby limiting the Bank's ability to perform risk-based monitoring; and (iii) as detailed in the CDD section above, Bank of America recognized that these customers posed elevated risks and were heavy users of negotiable instruments, yet the Bank did not account for such customers' use of this product in quarterly reviews of these customers' activities.

FinCEN's analysis concluded that between October 2020 and May 2025, Customers A and B received more than 680,000 individual transactions forming approximately 220,000 unique groups of suspicious deposits totaling over \$660 million, with these groups of three instruments bearing red flags including: (i) round dollar amounts; (ii) sequential numbering patterns; (iii) repeated groups of sequential money orders totaling between \$2,900 and \$3,000; and (iv) with respect to roughly one-in-three of these groups, purchase locations with a nexus to the southwest border. The map below reflects the total dollar volume of money orders deposited into the accounts

---

<sup>47</sup> The majority of these money orders were purchased at MSBs by individuals purchasing vehicles through the auction platforms maintained by Customers A and B, which money orders were then deposited by Customers A and B into their accounts at Bank of America.

of Customers A and B by purchase location from October 2020 to May 2025,<sup>48</sup> demonstrating that a significant amount of money orders originated from the southwest border, a pattern consistent with structuring designed to evade reporting thresholds while facilitating potential illicit proceeds and inconsistent with the geographic footprints of the relevant customers.



This repeated pattern throughout the Relevant Time Period was notable for three reasons. *First*, the repeated purchases of three sequential money orders totaling just under \$3,000 is a red flag that the purchasers were undertaking efforts to evade the identification and verification requirements imposed on the issuing MSBs, which apply to money orders of \$3,000 or more.<sup>49</sup> FinCEN has issued guidance highlighting that sequential purchases of monetary instruments may

<sup>48</sup> The map also includes a small amount of negotiable instrument deposits made by a third online auto auction customer that the Bank offboarded relatively early within the Relevant Time Period; although this customer's negotiable instrument deposits also exhibited similar patterns as those of Customers A and B, they are not included in the SAR violations described above as they contributed a relatively *de minimis* amount of the total suspicious activity.

<sup>49</sup> 31 CFR § 1010.415(a): "No financial institution may issue or sell a bank check or draft, cashier's check, money order or traveler's check for \$3,000 or more in currency unless it maintains records... which must be obtained for each issuance or sale... to any individual purchaser which involves currency in amounts of \$3,000-\$10,000." As noted above, the majority of money orders deposited by Customers A and B were purchased at MSBs.

be indicative of money laundering.<sup>50</sup> *Second*, the deposits of money orders that had been purchased from other financial institutions indicated that a high volume of negotiable instruments deposited into the accounts of Customers A and B were purchased by buyers of vehicles who behaved in a manner that suggested an attempt to evade identification and verification requirements.

*Third*, a material portion of this activity occurred even after Bank of America received warnings of potential money laundering risks.

In September 2021, Bank of America received a request for information from another financial institution regarding dozens of suspicious money order transactions deposited into accounts held by Customer B between July and August 2021. Despite this inquiry flagging the unusual money order activity, the Bank’s response indicated that it had identified no increase in money order transactions, no unusual velocity patterns, and no indicators of illicit activity. FinCEN’s investigation concluded that roughly 51,000 of the groups—or more than 23%—of suspicious deposits were processed for Customer B between October 2021 and May 2025 without timely reporting to FinCEN.

By September 2022, compliance personnel had recommended closing the accounts for Customer A—including because compliance personnel identified the risks associated with Customer A’s acceptance of third-party payments and the lack of transparency associated with the source of funds; the Bank ultimately did not adopt this recommendation and waited two years to begin restricting this and certain other customers’ use of money order deposits. FinCEN’s investigation concluded that roughly 72,000 of the groups—or more than 30%—of suspicious

---

<sup>50</sup> See FinCEN, [In re: Great Eastern Bank of Florida \(No. 2002-02\)](#) (Sept. 4, 2002); “[Guidance on Interpreting Financial Institution Policies in Relation to Recordkeeping Requirements Under 31 C.F.R. 103.29](#)” (Nov. 2002).; FIN-2010, A001, “[Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering](#)” (Feb. 18, 2010).

deposits were processed for Customer A between September 2022 and May 2025 without timely reporting to FinCEN.

In November of 2023, one of these customers publicly disclosed it was under investigation by DOJ for potential violations of certain money laundering laws. As described above in the CDD section,<sup>51</sup> the Bank took no meaningful steps to apply enhanced monitoring to this customer's activities, including the high volumes of deposits of money orders, following this public disclosure. FinCEN's investigation concluded that roughly 11,000 of the groups—or more than 10%—of suspicious deposits associated with this customer were processed between November 2023 and May 2025 without timely reporting to FinCEN.

## **2. High-risk Jurisdiction Wires for Online Auto Auction Customers.**

Bank of America filed late SARs related to wire transfers with a nexus to high-risk jurisdictions that were inconsistent with customer risk profiles and expected business purposes. FinCEN's investigation identified nearly \$1 billion in suspicious wire transactions for which the Bank failed to timely and accurately file SARs. These wires primarily involved Georgia, Belarus, and other Commonwealth of Independent States (CIS) nations and reflected what the Bank itself detected as a substantial change in behavior for relevant accounts.

Most of this activity occurred contemporaneous with or following Russia's invasion of Ukraine in February 2022. Moreover, roughly 98% of the suspicious wire activity by dollar value was associated with customers in auto-related industries, with two customers, Customers A and C, accounting for more than \$850 million of these suspicious transactions. Compliance personnel were aware of certain of these transactions in late 2022, yet the Bank failed to file the first SAR (which covered only a small portion—roughly 10%—of this activity) until August 2023, with the

---

<sup>51</sup> See Section II.D.3, *supra*.

bulk of this activity not reported until a subsequent SAR was filed in June 2025, which occurred only after the Bank received certain requests for information from FinCEN.

Bank of America's failure to timely file SARs on this activity is especially significant for five reasons. *First*, simultaneous with the relevant activity, publicly available information identified potential sanctions evasion risks associated with the auto industry.<sup>52</sup> Additionally, much of this activity was processed after compliance personnel recommended offboarding one of these auto-related customers. Specifically, of the wire transfers identified in this investigation, more than 18,000 wires totaling approximately \$850 million were conducted in September 2022 or later, well after FinCEN issued public guidance on sanctions evasion risks and after internal compliance escalations.

*Second*, Bank of America performed quarterly client activity monitoring for certain of these customers contemporaneous with this activity taking place, but such reviews did not incorporate any geographic information about wires and were generally superficial in nature, resulting in the Bank failing to take a risk-based approach to its ongoing monitoring of these customers' activities.

*Third*, many of these wires bore clear indicia of third-party payments and were processed after Bank of America's compliance personnel had already identified such risks as grounds for the late 2022 recommendation to close accounts for Customer A, one of the top customers associated with this wire activity. Analysis of wire instructions revealed numerous instances where multiple distinct originators remitted funds for vehicle purchases and referenced the same buyer identification number issued by Customer A, thereby indicating that Customer A was accepting third-party payments not just through deposits of money orders but also from wires it received

---

<sup>52</sup> FinCEN, FIN-2022-Alert002, [Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and Their Family Members](#) (Mar. 16, 2022); FinCEN & Bureau of Industry and Security, FIN-2023-Alert004, [Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts](#) (May 19, 2023).

from originators with whom Customer A had no direct relationship. In representative cases, dozens of different originators sent wires totaling hundreds of thousands of dollars to individual buyer accounts, indicating a many-to-one originator pattern, with some wires also indicating that the funds were being sent to Customer A to be “stored” by Customer A—a further indication of transactional activity inconsistent with an apparent lawful purpose or reasonable explanation.

*Fourth*, Customer C, the customer associated with the greatest volume and value of suspicious wires, had a customer profile identifying it as a “small-medium” commercial customer with expected annual sales of \$1 to \$4 million. Yet during approximately a three-year period, this customer processed **over \$700 million in wires** involving high-risk jurisdictions.

*Finally*, FinCEN’s investigation identified that many of these wires demonstrated crossover with the suspicious negotiable instrument activity described above. Notably, certain buyer identification numbers appeared in both the wire transfer data and the negotiable instrument deposits, indicating the use of multiple payment channels to facilitate the same underlying suspicious activity.<sup>53</sup>

### 3. CMLNs

FinCEN’s investigation identified hundreds of millions of dollars in suspicious transactions indicative of CMLNs involving likely TBML that the Bank failed to timely and accurately report. The majority of this activity involved a group of Bank of America customers that purported to operate in the logistics or electronics industries, but whose transaction patterns bore clear indicia of suspicion and were inconsistent with legitimate commercial activity for such businesses.

---

<sup>53</sup> One buyer identification number is referenced in a wire that Customer A received from a UAE entity and is also referenced in a round-dollar money order purchased in the U.S.

These suspicious patterns included, but were not limited to: high volumes of back-to-back credit card purchases at major retailers and shipping companies inconsistent with customer profiles; regular, large-value ACH and bill pay transactions to pay off balances for credit cards issued by third-party financial institutions, including for cards in the name of third-party individuals for which there was no apparent commercial purpose; large wire transfers to counterparties in China with generic descriptions (*e.g.*, “for goods”) and no discernible business rationale; and substantial, repeated transfers to counterparties with no web presence operating from residential addresses, demonstrating an apparent lack of legitimate commercial purpose.

Despite these red flags, Bank of America failed to timely identify and report this suspicious activity. Many of these transactions were processed after the Bank made certain enhancements to EP’s threshold.

#### **4. Other Late SARs**

As referenced earlier, in connection with the Bank’s decision to decrease EP’s investigative threshold from 20 points to either 10 or 12 points, the Bank conducted a limited, one-time review of Event Groups with scores between the old 20-point threshold and revised values. This review resulted in the Bank filing over 8,000 SARs totaling approximately \$3.96 billion in unreported suspicious activity, including 34 of which had significant indicators for money laundering, including activity indicative of TBML involving co-mingled funds with high-risk country counterparties, correspondent wire activity involving a Russian petrochemical entity with sanctioned ownership and high-risk jurisdictions, and healthcare-related transactions exhibiting cash structuring and layering techniques consistent with benefit fraud schemes.

### III. VIOLATIONS

FinCEN has determined that Bank of America willfully violated the BSA and its implementing regulations during the Relevant Time Period. Specifically, FinCEN has determined that the Bank willfully failed to implement and maintain an AML program that met the minimum requirements of the BSA, in violation of 31 U.S.C. § 5318 (h)(1) and 31 C.F.R. § 1020.210(a). Additionally, FinCEN determined that Bank of America willfully failed to conduct due diligence on correspondent accounts in the United States for foreign financial institutions, in violation of 31 U.S.C. § 5318(i) and 31 C.F.R. § 1010.610. FinCEN also determined that the Bank 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

As summarized below, FinCEN considered all factors outlined in the Statement on Enforcement of the Bank Secrecy Act issued August 18, 2020, when deciding whether to impose a civil money penalty in this matter.<sup>54</sup>

1. **Nature and seriousness of the violations, including extent of possible harm to the public and the amounts involved:** Bank of America's violations presented significant risk of serious harm to the U.S. financial system. During the Relevant Time Period the Bank's primary internal control for identifying and reporting suspicious transactions was not reasonably designed, including by allowing an increasing amount of suspicious activity to remain uninvestigated sufficiently or to be investigated only after an extended period of time (often, more than a year). Bank of America's own internal testing identified these

---

<sup>54</sup> FinCEN, [Financial Crimes Enforcement Network \(FinCEN\) Statement on Enforcement of the Bank Secrecy Act](#) (Aug. 18, 2020).

issues, yet the Bank failed to timely and adequately respond to them. As indicated in the examples in Section II.D.3, *supra*, the Bank failed to develop accurate risk profiles and to conduct risk-based ongoing monitoring for customers engaged in tens of billions of dollars' worth of transactions that Bank personnel had identified as such a serious concern that one customer engaged in this activity was initially recommended to be offboarded. These failures resulted in the Bank failing to timely report over \$5 billion in suspicious transactions, including more than \$1 billion of suspicious transactions that implicated significant U.S. national security-related and other priority illicit finance risks, such as suspicious transactions with indicia of CMLNs, fraud, and potential TBML with a nexus to the southwest border. This failure deprived law enforcement of timely and critical financial information pertaining to suspicious activity.

2. **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:** As a general matter, SARs represent one of the most important tools to FinCEN and law enforcement in fighting financial crime, both in proactively identifying potential illicit activity and in understanding the scope and scale of that illicit activity. FinCEN and law enforcement must be able to rely on financial institutions to remain vigilant and comply with their obligation to report suspicious activity, and Bank of America's violations caused a significant gap in the timely identification and reporting of suspicious activity. Bank of America's flawed approach to suspicious activity monitoring resulted in the Bank relying upon law enforcement inquiries and other manual processes to alert the Bank to potentially suspicious activity, with more than one-third of the Bank's investigations driven by "promotion" events—much of which consisted of outreach from law enforcement and

external stakeholders—rather than its own internal controls. Although a bank’s reasonable cooperation with law enforcement inquiries, participation in Section 314(b) information sharing, and employee referral processes remain important, the nature and extent of Bank of America’s reliance on those sources to alert it to relevant risks resulted in the Bank contravening two of the BSA’s key purposes:<sup>55</sup> the Bank’s failures materially increased the risks that money may have been laundered through the Bank and reduced the timely reporting of highly useful information to law enforcement. Critically, and as noted above, much of the suspicious activity that Bank of America failed to timely report implicated national security-related and other priority illicit finance risks, including suspicious activity indicative of CMLNs, fraud, and potential TBML with a nexus to the southwest border. Finally, the Bank’s flawed approach to suspicious activity reporting also undermined FinCEN’s ability to receive timely financial intelligence for analytical and investigative purposes, including its ability to disseminate such information to other financial institutions. FinCEN afforded greater weight to this factor given the nature and extent of the impact, including the potential implications for priority illicit finance risks.

**3. Pervasiveness of wrongdoing within an entity, including management’s complicity in, condoning or enabling of, or knowledge of the conduct underlying the violations:**

During the Relevant Time Period, Bank of America had numerous opportunities to correct the deficiencies identified by FinCEN’s investigation, including from findings of its own internal testing. Notably, given the Bank’s enterprise-wide application of EP and its reliance on EP as the primary control for identifying potentially suspicious activity, the associated deficiencies (and the compliance expenditures saved from meaningfully

---

<sup>55</sup> See 31 U.S.C. § 5311.

responding to them) necessarily spanned the Bank’s various business lines and were not, for example, cabined to a particular product or service. However, management focused on the impact to the Bank’s resourcing rather than remediation sufficient to address the relevant issues. As noted above, when this status quo was jeopardized by an unfavorable result from an internal test, the then-Global Head of Financial Crimes directed a senior manager to repeat the test at issue and achieved a more favorable result. Similarly, despite compliance personnel squarely identifying third-party payments as a core risk involving multiple high-risk customers initially recommended for offboarding, Bank of America prioritized the revenue associated with these customer relationships by accepting such customers’ continued engagement in the activity of concern without any changes to its approach to the ongoing monitoring of their activities or customer risk profiles. By 2023, Bank of America’s then-BSA Officer and the head of the relevant line of business had been briefed on risks identified by compliance personnel, yet these risks persisted without commensurate controls after these internal escalations.

4. **History of similar violations or misconduct in general, including prior criminal, civil, and regulatory enforcement actions:** Bank of America has no prior enforcement history with FinCEN. A Bank affiliate, however, has been subject to two formal BSA-related actions by regulatory authorities in 2023 and 2026 by the Securities and Exchange Commission for failing to file SARs.<sup>56</sup> Additionally, the Bank and its affiliates have been the subject of other actions by regulators and criminal authorities, including supervisory and oversight failures.

---

<sup>56</sup> See Securities and Exchange Commission, 2023-128, “[SEC Charges Merrill Lynch and Parent Company for Failing to File Suspicious Activity Reports](#),” (Jul. 11, 2023); 3-22652, “[SEC Institutes Settled Order Against Merrill Lynch for Failing to File Suspicious Activity Reports](#),” (Jun. 29, 2026). The 2026 SEC action involved missed SARs attributable to issues with EP.

5. **Financial gain or other benefit resulting from, or attributable to, the violations:** As noted above, the Bank's failure to reasonably remediate identified deficiencies stemmed in part from its failure to devote adequate resources to case investigations. When Bank of America began remediating EP near the end of the Relevant Time Period, it estimated that investigative case volumes would double, thereby requiring the Bank to recruit an estimated 750 additional personnel and indicating that the Bank had likely saved hundreds of millions of dollars in compliance-related expenditures during the Relevant Time Period. Separately, the Bank made the decision to retain high-risk and high-value customers despite recommendations to the contrary from compliance. FinCEN afforded greater weight to this factor given the duration and extent of the financial gain, including the substantial savings in compliance expenditures that the Bank was able to forego incurring as a result of its violations.
6. **Presence or absence of prompt, effective action to terminate the violations upon discovery, including self-initiated remedial measures:** During the Relevant Time Period, Bank of America had numerous opportunities to correct the deficiencies in its AML program, including based on findings of its own internal testing. However, the Bank's approach of making incremental changes that prioritized minimizing the impact on resourcing resulted in Bank of America allowing a significant number of suspicious transactions to go uninvestigated and/or unreported for prolonged periods of time. Ultimately, the Bank began to address certain deficiencies only after FinCEN began its investigation and extensive engagement with the Bank's Federal functional regulators.
7. **Timely and voluntary disclosure of the violations to FinCEN:** FinCEN's investigation was proactive and was not the result of voluntary disclosures made by Bank of America.

8. **Quality and extent of cooperation with FinCEN and other relevant agencies, including as to potential wrongdoing by its directors, officers, employees, agents, and counterparties:** Although Bank of America made dozens of productions of materials responsive to FinCEN's requests for information, these productions were often the subject of unreasonable delays, and the effectiveness of such cooperation was also limited in other respects. The Bank undertook no proactive investigation of the historical activity of concern to FinCEN and the focus of FinCEN's investigation. The Bank also failed to timely produce responsive materials to a set of FinCEN requests, thereby hindering the efficiency of FinCEN's investigative process.
9. **Systemic Nature of the Violations. Considerations include, but are not limited to, the number and extent of violations, failure rates (e.g., the number of violations out of total number of transactions), and duration of violations:** Bank of America is the second-largest bank in the United States and as such, it processes a significant volume of transactions. Bank of America's willful violations of the BSA during the Relevant Time Period were systemic and implicated multiple core aspects of its AML program. As detailed above, the Bank's transaction monitoring system had been in place for many years, yet the Bank began to make responsive changes only near the end of the Relevant Time Period. As also detailed above, this system had significant gaps, including the failure to provide for any automated monitoring of negotiable instrument deposits despite tens of billions of dollars in such activity by customers that, during the Relevant Time Period, compliance personnel identified as posing elevated risks to the Bank. Such automated monitoring deficiencies and gaps were exacerbated by deficiencies in certain of the Bank's CDD processes, including the Bank's failure to timely and reasonably respond to concerns

raised by compliance personnel that implicated the risk profiles of the relevant customers. FinCEN afforded greater weight to this factor given the duration that the issues persisted and the magnitude of the impact that resulted, including due to the Bank's size and volume of financial activity.

**10. Whether another agency took enforcement action for related activity. FinCEN will consider the amount of any fine, penalty, forfeiture, and/or remedial action ordered:**

Following a separate but parallel investigation led by the OCC, Bank of America has agreed to pay \$750,000,000 to resolve this investigation. The Office of Foreign Assets Control also conducted a separate investigation resulting in the assessment of an \$11,000,000 penalty.

**V. CIVIL PENALTY**

FinCEN may impose a Civil Money Penalty of up to \$71,545 per day for willful violations of the requirement to implement and maintain an AML program.<sup>57</sup> For each willful violation of the SAR reporting requirement, FinCEN may impose a civil money penalty not to exceed the greater of the amount involved in the transaction (but capped at \$286,184) or \$71,545.<sup>58</sup> For each willful violation of the requirement to implement a risk-based due diligence program for correspondent accounts established, maintained, administered, or managed in the United States for foreign financial institutions, FinCEN may impose a civil money penalty "in an amount equal to not less than two (2) times the amount of the transaction," but not more than \$1,776,364.<sup>59</sup>

After considering all the facts and circumstances, as well as the enforcement factors discussed above, FinCEN is imposing a Civil Money Penalty of \$1,200,000,000 in this matter.

---

<sup>57</sup> 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

<sup>58</sup> 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

<sup>59</sup> 31 U.S.C. § 5321(a)(7); 31 C.F.R. § 1010.821.

FinCEN has agreed to credit against the Civil Money Penalty payment of \$750,000,000 to the OCC. Accordingly, Bank of America shall make payment of \$450,000,000 to the Department of the Treasury pursuant to the payment instructions that will be transmitted to Bank of America upon execution of this Consent Order.

## **VI. UNDERTAKINGS**

The undertakings agreed to in this Consent Order are in addition to, and independent of, any undertakings to which the Bank or its affiliates agree in connection with any related consent order, settlement agreement, or any other agreements with or orders imposed by any other representative of the United States or agencies thereof.<sup>60</sup> For purposes of Section VI, references to “independent” means that the qualified consultant and any affiliate thereof did not, prior to December 2024, provide services to Bank of America or an affiliate thereof regarding the design and implementation of the Bank’s AML Program that are the subject of the Undertakings set forth in this Section VI.

Pursuant to the December 2024 Cease and Desist Order from the OCC, Bank of America is required to engage qualified independent consultants to conduct various reviews, including of certain historical activity to determine whether SARs should be filed. Bank of America may propose to FinCEN that such previously engaged consultants may serve as the SAR Lookback Consultant (described below) and that transactions previously reviewed pursuant to such lookbacks be taken into account, as appropriate, in determining the scope and methodology of the SAR Lookback Review, subject to FinCEN’s review of the scope, methodology, and results of such prior reviews. In addition, and subject to FinCEN approval, any such consultant may also

---

<sup>60</sup> Upon request, the OCC may receive copies of all reports referenced in Sections VI.A through VI.D.

serve as the independent consultant for one or more Undertakings required under Sections VI.B, VI.C, or VI.D.

By execution of this Consent Order, Bank of America agrees to the following Undertakings:

**A. SAR Lookback**

1. Within 60 days of execution of this Consent Order, Bank of America shall propose a qualified independent consultant (SAR Lookback Consultant) that the Bank intends to hire within 30 days (at its own expense) to conduct a SAR Lookback Review. FinCEN has the right to veto the engagement of a SAR Lookback Consultant that FinCEN deems unsuitable to complete the SAR Lookback Review. The SAR Lookback Consultant will determine whether activity effected by Bank of America's customers from January 2022 until the completion of Bank of America's remediation of issues related to its suspicious activity monitoring processes (including, but not limited to, deficiencies and gaps in EP, its feeder models, and related investigative processes), is properly identified and reported under 31 U.S.C. § 5318(g) and implementing regulations, including but not limited to: (i) activity involving credit cards (including payments that Bank of America received from accounts maintained at third-party financial institutions related to balances associated with credit cards issued by Bank of America as well as payments made by Bank of America customers to third-party financial institutions related to balances associated with credit cards issued by such third-party financial institutions); (ii) negotiable instruments (including deposits of negotiable instruments purchased at third-party financial institutions); (iii) cross-border wire and other transactions with a nexus to high-risk jurisdictions, including those jurisdictions with a greater risk of implicating the Priority Illicit Finance Risks described below; and (iv) Event Groups that were not previously investigated because they fell between 10 or 12 points (as

applicable) and 20 points, with the SAR Lookback Consultant to consider targeted expansions to Event Groups scoring between 6-10 points subject to risk-based analytical methodologies (collectively, Covered Transactions).<sup>61</sup>

2. The SAR Lookback Consultant's review of Covered Transactions will follow a risk-based approach, including by prioritizing the review of transactions with potential ties to the following risks: (i) the U.S. Southwest border, cartels, and possible narcotics trafficking; (ii) CMLNs; (iii) Iran; and (iv) Russia (Priority Illicit Finance Risks). The SAR Lookback Consultant will consider, and as appropriate in the Consultant's discretion, apply advanced approaches to identify potentially suspicious transactions from the full population of Covered Transactions warranting investigation, including: (i) super intelligence models,<sup>62</sup> (ii) graph analytics or other network analysis tools, and (iii) segmentation based on the relevant customer, product or service, geographic region, or channel associated with the activity.

3. Within 150 days from the date of engagement, the SAR Lookback Consultant will deliver to FinCEN a report summarizing the proposed scope and methodology of the review of the Covered Transactions that the SAR Lookback Consultant plans to conduct (SAR Lookback Scope Report). FinCEN, in consultation with the SAR Lookback Consultant, may amend the scope of the review of Covered Transactions within 30 days of FinCEN's receipt of the SAR Lookback Scope Report. Bank of America will grant the SAR Lookback Consultant access to all appropriate systems and records reasonably necessary to conduct the SAR Lookback Review. Following

---

<sup>61</sup> Such risk-based analytical methodologies may include: (i) extension of graph analytics or network analysis beginning with customers exhibiting known risk factors, (ii) supervised super intelligence models to identify highest priority risk factors or signals, and (iii) tiering based on customer risk profiles and identified risk factors.

<sup>62</sup> The SAR Lookback Consultant may, in its discretion, initially use an unsupervised model in exploratory or preliminary aspects of the SAR Lookback Review but, to the extent super intelligence is used to identify potentially suspicious activity from the broader universe of Covered Transactions, the Consultant will apply a supervised model (including based on labeled data from relevant Bank transactions).

submission of the SAR Lookback Scope Report to FinCEN, the SAR Lookback Consultant will deliver quarterly progress reports to FinCEN documenting the status of the SAR Lookback Review. Based on the quarterly progress reports, FinCEN, in consultation with the SAR Lookback Consultant, may expand the period or scope of the SAR Lookback Review within the Relevant Time Period.

4. Within eighteen months from the date of the SAR Lookback Scope Report, and no later than December 2028, the SAR Lookback Consultant will deliver a detailed report (SAR Lookback Report) to FinCEN and Bank of America that summarizes the methodology and findings of its review and identifies the Covered Transactions that may, pursuant to the process outlined below, require a SAR to be filed pursuant to 31 U.S.C. § 5318(g) and its implementing regulations. Bank of America will make, and will cause the SAR Lookback Consultant to make, interim reports, drafts, work papers, or other supporting materials related to the SAR Lookback Review available to FinCEN upon request. Bank of America will comply with the findings of the SAR Lookback Consultant or FinCEN that Bank of America file SARs on any of the Covered Transactions, and, in the event that either of the SAR Lookback Consultant or FinCEN recommend that the Bank file a SAR on a Covered Transaction, Bank of America will comply with that recommendation. Bank of America may begin filing SARs on the Covered Transactions during the pendency of the SAR Lookback Review (and prior to completion of the SAR Lookback Report), provided that the Bank notifies FinCEN at least 30 days prior to commencing such SAR filings.

5. No later than 90 days from the date of the SAR Lookback Report, Bank of America will complete the filing with FinCEN of SARs regarding all the Covered Transactions identified by the SAR Lookback Consultant as ones that would have required a report pursuant to 31 U.S.C. § 5318(g) and its implementing regulations.

**B. Effectiveness Testing of Suspicious Activity Monitoring Processes (including Responsible Innovation)**

6. Within 30 days of execution of this Consent Order, Bank of America shall propose a qualified independent consultant (Suspicious Activity Monitoring Consultant) to hire within 30 days (at its own expense) to test the effectiveness of the Bank's suspicious activity monitoring internal policies, procedures, and controls within two intervals: (i) with respect to testing the effectiveness of interim controls applied by the Bank while remediation of EP and related systems and processes remains ongoing (Interim Controls Review), commencement of such review within 7 days of the Suspicious Activity Monitoring Consultant's submission of the Interim Controls Review Scope Report (as detailed below) and completion of such review within 60 days of the Scope Report submission; and (ii) with respect to the Bank's revised approach to suspicious activity monitoring (End State Effectiveness Review), commencement of such review within 60 days of the Bank notifying the Suspicious Activity Monitoring Consultant and FinCEN that such remediation is complete (but in no case will such testing commence later than October 2027) and completion of such review within 240 days of the Consultant commencing such review.

7. FinCEN has the right to veto the engagement of a Suspicious Activity Monitoring Consultant deemed unsuitable to complete either of the Interim Controls or End State Reviews. Bank of America will make, and will cause the Suspicious Activity Monitoring Consultant to make, interim reports, drafts, work papers or other supporting materials related to the Internal Controls and End State Effectiveness Reviews available to FinCEN upon request.

### Interim Controls Review

8. The Interim Controls Review will assess the sufficiency of interim controls with respect to the Bank's obligation to timely identify and report suspicious transactions under 31 C.F.R. § 1020.320.

9. Within 30 days of Bank of America's retention of the Suspicious Activity Monitoring Consultant, the Consultant will submit to FinCEN a report summarizing the proposed scope and methodology of the Interim Controls Review (Interim Controls Review Scope Report).

10. Within the Interim Controls Review Scope Report, the Suspicious Activity Monitoring Consultant will explain how it plans to identify and assess the effectiveness of any of Bank of America's interim controls to fulfill the Bank's obligation to timely identify and report suspicious transactions under 31 C.F.R. § 1020.320 by setting forth the parameters of a risk-based review that focuses on: (i) known gaps or deficiencies with EP, its feeder models, or related investigative processes that have not yet been remediated, (ii) transaction testing to assess the likelihood that any such gaps or deficiencies may implicate one or more Priority Illicit Finance Risks, and (iii) to the extent such testing identifies a reasonable likelihood that such gaps or deficiencies may implicate one or more Priority Illicit Finance Risks, the magnitude of such impact. FinCEN, in consultation with the Suspicious Activity Monitoring Consultant, may amend the scope of Interim Controls Review within 15 days of FinCEN's receipt of the Interim Controls Review Scope Report. Bank of America will grant the Suspicious Activity Monitoring Consultant access to all appropriate systems and records reasonably necessary to conduct the Interim Controls Review.

11. Within 15 days of completing the Interim Controls Review, the Suspicious Activity Monitoring Consultant will submit to FinCEN a written report: (i) addressing the overall

effectiveness of Bank of America’s interim controls related to suspicious activity monitoring, (ii) describing the review performed—including, at a minimum, the sampling methodology, number of customers, and amount of transactional activity evaluated as part of the review (including the number of customers and amount of transactional activity evaluated because of a potential nexus to Priority Illicit Finance Risks); and (iii) describing any recommended actions to address the findings of the Interim Controls Review, including: (A) focus areas within the SAR Lookback Review described in Section VI.A, *supra*, and (B) recommendations for changes to, or the addition of new interim controls, which may include manual processes, manual periodic reviews, product-driven analyses, or any risk-based changes for the Bank to apply while its remediation of suspicious activity monitoring policies, procedures, and controls remains ongoing.

12. Within 15 days of receiving the Interim Controls Review Report, Bank of America will develop a plan to implement any recommendations made in the Interim Controls Review Report or, within 15 days after issuance of a report, propose alternatives. The Suspicious Activity Monitoring Consultant will provide a written response to any proposed alternatives within 15 days.

#### End State Effectiveness Review

13. Within 30 days of the Bank notifying the Suspicious Activity Monitoring Consultant and FinCEN that such remediation is complete (but in no case later than September 2027), the Suspicious Activity Monitoring Consultant will submit to FinCEN a report summarizing the proposed scope and methodology of the End State Effectiveness Review (End State Effectiveness Review Scope Report).<sup>63</sup> At a minimum, the testing associated with the End State

---

<sup>63</sup> If the Suspicious Activity Monitoring Consultant determines that significant transaction monitoring remediation measures will be delayed beyond July 30, 2027, the Suspicious Activity Monitoring Consultant may request an alternative timeline to begin the End State Effectiveness Review upon completion of these measures through the provision of a written request, including the justification for the alternative timeline, to FinCEN. In its discretion, FinCEN may provide an extension for the commencement of the End State Effectiveness Review as well as corresponding revisions to the deadline for providing the Scope and final reports.

Effectiveness Review should occur at two different times: (i) an initial review to inform and highlight remaining gaps and deficiencies associated with the Bank's suspicious activity monitoring, and (ii) following Bank of America's execution of the steps set forth in the Implementation Plan described below, a subsequent review to validate the effectiveness in meaningfully mitigating the relevant risks of any enhancements Bank of America makes in connection with the End State Effectiveness Review. The Suspicious Activity Monitoring Consultant will measure the results of such testing using objective criteria to determine the Bank's compliance with the BSA and its implementing regulations, including but not limited to the degree of Bank of America's adherence to its internal policies, procedures, and controls.

14. Within the End State Effectiveness Review Scope Report, the Suspicious Activity Monitoring Consultant will explain how it plans to identify and assess the effectiveness of Bank of America's revised approach to suspicious activity monitoring to fulfill the Bank's obligation to timely identify and report suspicious transactions under 31 C.F.R. § 1020.320 by setting forth the parameters of a risk-based review that focuses on: (i) the effectiveness of models (including EP's feeder models) in identifying potentially suspicious activity; (ii) the effectiveness of risk factor weights or similar scoring methodologies in reflecting relevant risks; (iii) the effectiveness of investigative processes, including the adequacy of investigations in accurately, completely, and timely reviewing potentially suspicious transactions warranting investigation; (iv) the overall effectiveness of the Bank's revised approach to suspicious activity monitoring in mitigating relevant risks identified through the Bank's risk assessment processes; (v) the effectiveness of the Bank's approach to testing its suspicious activity monitoring, including the appropriateness and timeliness of the Bank's corrective actions in response to the findings of such internal testing; (vi) the consistency of the performance of the Bank's suspicious activity monitoring; (viii) the

sustainability of the Bank’s suspicious activity monitoring, including the sufficiency of personnel and technological resources as well as governance frameworks to ensure such monitoring (including any overrides, whitelists, or similar exceptions) remains risk-based, explainable, and subject to appropriate Bank oversight; and (ix) the degree to which the Bank’s use of responsible innovation is effective in timely identifying and reporting transactions with a nexus to Illicit Finance Priority Risks. The End State Effectiveness Review Scope Report will explain the Suspicious Activity Monitoring Consultant’s planned use of transaction testing to assess the likelihood that any identified issues implicate one or more Priority Illicit Finance Risks, and to the extent such testing identifies a reasonable likelihood of one or more Priority Illicit Finance Risks being implicated, the magnitude of such impact.

15. FinCEN, in consultation with the Suspicious Activity Monitoring Consultant, may amend the scope of the End State Effectiveness Review within 30 days of FinCEN's receipt of the End State Effectiveness Review Scope Report. Bank of America will grant the Suspicious Activity Monitoring Consultant access to all appropriate systems and records reasonably necessary to conduct the End State Effectiveness Review.

16. Within 45 days of completing the End State Effectiveness Review but no later than July 2028, the Suspicious Activity Monitoring Consultant will submit to FinCEN a written report:

- (i) addressing the overall effectiveness of Bank of America’s suspicious activity monitoring,
- (ii) describing the review performed—including, at a minimum, the sampling methodology, number of customers, and amount of transactional activity evaluated as part of the review (including the number of customers and amount of transactional activity evaluated because of a potential nexus to Priority Illicit Finance Risks);
- (iii) detailing any identified deficiencies or gaps, including any recommended actions to address such deficiencies or gaps as well as the likelihood

that such deficiency or gap may impact one or more Priority Illicit Finance Risks as well as the magnitude of such impact.

17. Bank of America will develop a plan to implement any recommendations made in connection with the End State Effectiveness Review (End State Remediation Plan) or, within 90 days after issuance of a report, propose alternatives. The Suspicious Activity Monitoring Consultant will provide a written response to the End State Remediation Plan, including any proposed alternatives, within 60 days. Within 180 days after finalization of the End State Remediation Plan, the Suspicious Activity Monitoring Consultant will provide FinCEN with a written report detailing the extent to which Bank of America has adopted and implemented the End State Remediation Plan, including, but not limited to specific changes that the Suspicious Activity Monitoring Consultant verified that Bank of America made to its suspicious activity monitoring in response to the End State Effectiveness Review.

#### **C. Effectiveness Testing of CDD and Foreign Correspondent Account Due Diligence Program**

18. Within 60 days of execution of this Consent Order, Bank of America shall propose a qualified independent consultant (CDD and Foreign Correspondent Due Diligence Program Consultant) to hire within 30 days (at its own expense), to test the effectiveness of the Bank's: (i) customer due diligence, including internal policies, procedures, and controls to sufficiently understand the nature and purpose of customer relationships for purposes of developing customer risk profiles as well as those to conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, to maintain and update customer information (CDD Review); and (ii) due diligence program applicable to correspondent accounts established, maintained, administered, or managed by the Bank for a foreign financial institution (including, but not limited to, the Bank's foreign branches and affiliates), including policies, procedures, and controls to

enable the covered financial institution to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any such correspondent account (Foreign Correspondent Account Due Diligence Program Review).

19. FinCEN has the right to veto the engagement of a CDD and Foreign Correspondent Due Diligence Program Consultant deemed unsuitable to complete either of the CDD or Foreign Correspondent Account Due Diligence Program. Bank of America will make, and will cause the CDD and Foreign Correspondent Due Diligence Program Consultant to make, interim reports, drafts, work papers or other supporting materials related to the CDD and Foreign Correspondent Account Due Diligence Reviews available to FinCEN upon request.

#### CDD Review

20. Within 90 days of the Bank's retention of the CDD and Foreign Correspondent Due Diligence Program Consultant, the Consultant will submit to FinCEN a written report summarizing the proposed scope and methodology of the CDD Review (CDD Scope Report). Such methodology must include risk-based testing of the Bank's high-risk customers, with the determination of the in-scope population for such testing to be in the discretion of the CDD and Foreign Correspondent Due Diligence Program Consultant, in consultation with FinCEN, which may provide to the CDD and Foreign Correspondent Due Diligence Program Consultant, prior to the CDD Scope Report deadline, a list of specific accounts that must be included in the in-scope population for the risk-based testing of Bank of America's high-risk customers. The Bank will grant the CDD and Foreign Correspondent Due Diligence Program Consultant access to all appropriate systems and records reasonably necessary to identify the in-scope population for such testing. In undertaking such testing, as well as approaching the CDD Review more broadly, the Consultant will prioritize customers and transactions with potential ties to Priority Illicit Finance

Risks. For purposes of determining the in-scope population, the CDD and Foreign Correspondent Due Diligence Program Consultant may, in its discretion, primarily select samples from customers that the Bank rated as high and higher risk, provided that such sample is supplemented with additional customers that the CDD and Foreign Correspondent Due Diligence Program Consultant identifies from populations that the Bank rated as medium and low risk.

21. At a minimum, such testing should occur at two different times during the CDD Review: (i) an initial review to inform and highlight instances potential gaps and deficiencies associated with the Bank's CDD internal policies, procedures, and controls, and (ii) following Bank of America's execution of the steps set forth in the Implementation Plan described below, a subsequent review to validate the effectiveness in meaningfully mitigating the relevant risks of any enhancements Bank of America makes in connection with the CDD Review. The CDD and Foreign Correspondent Due Diligence Program Consultant will measure the results of such testing using objective criteria to determine the Bank's compliance with the BSA and its implementing regulations, including but not limited to the degree of Bank of America's adherence to its current CDD internal policies, procedures, and controls. Additionally, the CDD Scope Report must include proposed analyses to cover the following aspects:

- a. **Customer Risk Profiles:** whether Bank of America develops and maintains customer risk profiles consistent with the requirements of 31 CFR 1020.210(a)(2)(v), including by ensuring that, through applicable internal policies, procedures, and controls, the Bank incorporates and adjudicates in such risk profiles information regarding: (i) the nature and purpose of the customer relationship and material financial crime risks identified during the course of that relationship, including the products and services materially used by the customer and the expected nature, volume, value, and

geographic scope of customer activity; (ii) information obtained through transaction monitoring alerts and investigations, law enforcement and regulatory inquiries, requests for information from other financial institutions concerning potentially suspicious activity, and other relevant sources; and (iii) material commercial or transactional relationships with other customers, counterparties, or affiliated or unaffiliated entities, where such relationships are relevant to understanding the customer's risk profile.

- b. **Ongoing Monitoring of Customer Activity:** whether Bank of America conducts ongoing monitoring of customer activity to timely identify and report suspicious transactions in a manner consistent with the requirements of 31 CFR 1020.210(a)(2)(v), including, as applicable: (i) whether such monitoring is appropriately informed by the relevant aspects of the customer risk profile, including processes to identify and address material deviations between expected and actual activity—such as changes in transactional volume, value, products, counterparties, or geographic activity—particularly in response to emerging or evolving risks associated with the relevant geographic regions; (ii) whether material information identified through ongoing monitoring—including transaction monitoring alerts and investigations, requests for information from other financial institutions concerning potentially suspicious activity, and other information indicating heightened or changing customer risk—is timely assessed and, where appropriate, incorporated into the Bank's monitoring of subsequent customer activity; (iii) whether, when Bank personnel identify material risks or connections among customers or counterparties, the Bank properly uses such information to inform its ongoing monitoring; and, (iv) whether material changes in

customer activity or risk, including risks identified by compliance personnel, are timely escalated and resolved and result, where appropriate, in updates to customer information, monitoring, or other risk-based measures.

22. FinCEN may amend the scope of the CDD Review by providing written notice to the Bank 30 days after FinCEN's receipt of the CDD Scope Report.

23. Within 60 days following completion of the CDD Review, but no later than one year from the date of the CDD and Foreign Correspondent Due Diligence Program Consultant's engagement, absent prior written approval from FinCEN, the Consultant will submit to FinCEN a written report (the CDD Review Report) (i) addressing the overall effectiveness of the aspects of the Bank's CDD internal policies, procedures, and controls identified in the CDD Scope Report; (ii) describing the review performed, including the sampling methodology, number and risk classifications of customers and correspondent accounts reviewed, relevant transactional activity evaluated, and the number of customers, accounts, and transactions reviewed because of a potential nexus to Priority Illicit Finance Risks; and (iii) detailing any identified deficiencies or gaps, including any recommended actions to address such deficiencies or gaps as well as the likelihood that such deficiency or gap may impact one or more Priority Illicit Finance Risks as well as the magnitude of such impact. The Bank will make, and will cause the CDD and Foreign Correspondent Due Diligence Program Consultant to make, interim reports, drafts, work products, testing results, and other supporting materials related to the CDD Review Report available to FinCEN upon request.

24. Bank of America, in consultation with the CDD and Foreign Correspondent Due Diligence Program Consultant, will develop a written plan to implement any recommendations made in connection with the CDD Review Report and the Consultant's recommendations (CDD

Implementation Plan) or, within 90 days after issuance of a report, propose alternatives. The CDD and Foreign Correspondent Due Diligence Program Consultant will provide a written response to any proposed alternatives within 60 days.

25. Within 180 days following completion of the End State Effectiveness Review, or such other period approved in writing by FinCEN, the CDD and Foreign Correspondent Due Diligence Program Consultant will submit to FinCEN with a written report describing the extent to which the Bank has implemented the Implementation Plan and verify the effectiveness of material changes made in response to the review, including, as applicable, enhanced monitoring, additional controls, restrictions on products or services, or other risk mitigation measures.

#### Foreign Correspondent Account Due Diligence Program Review

26. Within 90 days of the Bank's retention of the CDD and Foreign Correspondent Due Diligence Program Consultant, the Consultant will submit to FinCEN a written report summarizing the proposed scope and methodology of the Foreign Correspondent Account Due Diligence Program Review (the Foreign Correspondent Account Due Diligence Scope Report). Such methodology must include risk-based testing of the Bank's high-risk foreign financial institution customers (including the Bank's own foreign branches and affiliates), with the determination of the in-scope population for such testing to be in the discretion of the CDD and Foreign Correspondent Due Diligence Program Consultant, in consultation with FinCEN, which may provide to the CDD and Foreign Correspondent Due Diligence Program Consultant, prior to the Foreign Correspondent Account Due Diligence Scope Report deadline, a list of specific accounts that must be included in the in-scope population for the risk-based testing of Bank of America's high-risk customers. The Bank will grant the CDD and Foreign Correspondent Due Diligence Program Consultant access to all appropriate systems and records reasonably necessary to identify

the in-scope population for such testing. In undertaking such testing, as well as approaching the Foreign Correspondent Account Due Diligence Program Review more broadly, the Consultant will prioritize customers and transactions with potential ties to Priority Illicit Finance Risks. For purposes of determining the in-scope population, the CDD and Foreign Correspondent Due Diligence Program Consultant may, in its discretion, primarily select samples from customers that the Bank rated as high and higher risk, provided that such sample is supplemented with additional customers that the CDD and Foreign Correspondent Due Diligence Program Consultant identifies from populations that the Bank rated as medium and low risk.

27. At a minimum, such testing should occur at two different times during the Foreign Correspondent Account Due Diligence Program Review: (i) an initial review to inform and highlight instances potential gaps and deficiencies associated with the Bank's due diligence program for correspondent accounts for foreign financial institutions; and (ii) following Bank of America's execution of the steps set forth in the Implementation Plan described below, a subsequent review to validate the effectiveness in meaningfully mitigating the relevant risks of any enhancements Bank of America makes in connection with the Foreign Correspondent Due Diligence Review. The CDD and Foreign Correspondent Due Diligence Program Consultant will measure the results of such testing using objective criteria to determine the Bank's compliance with the BSA and its implementing regulations, including but not limited to the degree of Bank of America's adherence to its current due diligence program for correspondent accounts for foreign financial institutions. Additionally, the Foreign Correspondent Account Due Diligence Program Report must include proposed analyses to cover risk-based testing of the Bank's due diligence program for correspondent accounts maintained for foreign financial institutions, including controls designed to comply with 31 U.S.C. 5381(l) and 31 C.F.R. § 1010.610. The CDD and

Foreign Correspondent Due Diligence Program Consultant shall prioritize review of (i) foreign branches and affiliates for which the Bank maintains correspondent relationships; and (ii) other respondent institutions presenting a greater likelihood of exposure to Priority Illicit Finance Risks—including, with respect to potential Iran-related exposure, accounts for foreign financial institutions based or with branches in countries presenting an elevated risk for Iran-related sanctions evasion, including through the use of proxies and facilitators located outside Iran. The review shall assess whether the Bank appropriately identifies, documents, evaluates, and responds to the money laundering, terrorist financing, sanctions evasion, and other illicit finance risks presented by such relationships, including whether customer due diligence and ongoing monitoring are reasonably designed to identify and respond to transactional patterns indicative of attempts to obscure the source, destination, or purpose of funds, including structuring, smurfing, reverse structuring or smurfing, and other patterns associated with illicit procurement or sanctions evasion.

28. FinCEN may amend the scope of the Foreign Correspondent Account Due Diligence Review by providing written notice to the Bank 30 days after FinCEN's receipt of the Foreign Correspondent Account Due Diligence Scope Report.

29. Within 60 days following completion of the Foreign Correspondent Account Due Diligence Review, but no later than one year from the date of the CDD and Foreign Correspondent Due Diligence Program Consultant's engagement, absent prior written approval from FinCEN, the Consultant will submit to FinCEN a written report (the Foreign Correspondent Account Due Diligence Review Report) (i) addressing the overall effectiveness of the aspects of the Bank's due diligence program for correspondent accounts for foreign financial institutions identified in the Foreign Correspondent Account Due Diligence Scope Report; (ii) describing the review

performed, including the sampling methodology, number and risk classifications of customers and correspondent accounts reviewed, relevant transactional activity evaluated, and the number of customers, accounts, and transactions reviewed because of a potential nexus to Priority Illicit Finance Risks; and (iii) detailing any identified deficiencies or gaps, including any recommended actions to address such deficiencies or gaps as well as the likelihood that such deficiency or gap may impact one or more Priority Illicit Finance Risks as well as the magnitude of such impact;. The Bank will make, and will cause the CDD and Foreign Correspondent Due Diligence Program Consultant to make interim reports, drafts, work products, testing results, and other supporting materials related to the Foreign Correspondent Account Due Diligence Review Report available to FinCEN upon request.

30. Bank of America, in consultation with the CDD and Foreign Correspondent Due Diligence Program Consultant, will develop a written plan to implement any recommendations made in connection with the Foreign Correspondent Account Due Diligence Review Report and the Consultant's recommendations (Foreign Correspondent Account Due Diligence Implementation Plan) or, within 90 days after issuance of a report, propose alternatives. The CDD and Foreign Correspondent Due Diligence Program Consultant will provide a written response to any proposed alternatives within 60 days.

31. Within 180 days following completion of the End State Effectiveness Review, or such other period approved in writing by FinCEN, the CDD and Foreign Correspondent Due Diligence Program Consultant will submit to FinCEN a written report describing the extent to which the Bank has implemented the Implementation Plan and verify the effectiveness of material changes made in response to the review, including, as applicable, enhanced monitoring, additional controls, restrictions on products or services, or other risk mitigation measures.

#### **D. Data Governance Review of BSA/AML-Related Information**

32. Within 60 days of signing the Consent Order, Bank of America shall propose a qualified independent consultant (Data Governance Consultant) to hire within 30 days (at its own expense) to conduct a Data Governance Review. The Data Governance Review will assess the Bank's data governance framework (including implementing policies, procedures, and internal controls) applicable to information that the Bank uses or is otherwise required for use in its AML Program, including but not limited to information related to transaction monitoring for compliance with the Bank's obligation to identify and report suspicious transactions under 31 C.F.R. § 1020.320 and data and records necessary to comply with its recordkeeping obligations under 31 C.F.R. § 1020.410.

33. FinCEN has the right to veto the engagement of a Data Governance Consultant deemed unsuitable to complete the Data Governance Review. Bank of America will make, and will cause the Data Governance Consultant to make, interim reports, drafts, work papers or other supporting materials related to the Data Governance Review available to FinCEN upon request.

34. The Data Governance Review will assess Bank of America's data governance framework for accuracy, completeness, consistency, effectiveness, and timeliness of Bank of America's AML data processing, including relative to Bank of America's size, complexity, and risk profile. The Data Governance Consultant will review and make corresponding recommendations, including consideration of Bank of America's: (i) governing bodies, fora, and other structures responsible for the design, implementation, and oversight of the relevant policies, procedures, and internal controls; (ii) identification and definition of relevant stakeholders and their corresponding roles and responsibilities, including the maintenance of Bank personnel with the requisite subject matter expertise applicable to the in-scope data populations; (iii) identification

and flow of relevant data sources and associated systems; and (iv) controls and monitoring of the use of relevant data within its AML Program—both as currently designed and with respect to processes governing change- or issue-management—including quality control, assurance, and other error detection mechanisms.

35. Within 90 days of Bank of America’s retention of the Data Governance Consultant, the Data Governance Consultant will submit to FinCEN a report summarizing the proposed scope and methodology of the Data Governance Review. The Data Governance Review Consultant will deliver quarterly progress reports to FinCEN documenting the status of the Data Governance Review.

36. Within 60 days from the end of its review, but no later than one year from the date of its engagement, the Data Governance Review Consultant will submit to FinCEN a written report setting forth the Data Governance Review Consultant’s recommendations and completed remedial actions as well as commitments by Bank of America to revise the Bank’s data governance framework.

## **VII. CONSENT AND ADMISSIONS**

To resolve this matter and only for that purpose, Bank of America 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. The Bank 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. Bank of America 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, the Bank shall be precluded from disputing any fact or contesting any determinations set forth in this Consent Order.

To resolve this matter, Bank of America agrees to and consents to the issuance of this Consent Order and all terms herein and agrees to make payment of \$450,000,000 to the U.S. Department of the Treasury within ten days of the Effective Date of this Consent Order. If timely payment is not made, Bank of America agrees that interest, penalties, and administrative costs will accrue.<sup>64</sup>

Bank of America 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. Bank of America 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 the Bank'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.

Bank of America 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 the Bank to agree to or approve this Consent Order, except as specified in this Consent Order.

Bank of America understands and agrees that this Consent Order implements and embodies the entire agreement between Bank of America and FinCEN, and its terms relate only to this

---

<sup>64</sup> 31 U.S.C. § 3717; 31 C.F.R. § 901.9.

enforcement matter and any related proceeding and the facts and determinations contained herein. Bank of America further understands and agrees that there are no express or implied promises, representations, or agreements between the Bank 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.

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

Bank of America 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, Bank of America authorizes and agrees to accept all service of process and filings through the Notification procedures below and to waive formal service of process.

## **VIII. COOPERATION**

Bank of America 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. Bank of America 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 about which FinCEN may inquire of the Bank. Bank of America'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.

## **IX. 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 Bank of America 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 Bank of America 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 the Bank 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.

## **X. 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, Bank of America 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; and
- F. Any and all claims for fees, costs, or expenses related in any way to this enforcement matter, Consent Order, or any related administrative 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. Bank of America agrees to bear its own costs and attorneys' fees.

## **XI. VIOLATIONS OF THIS CONSENT ORDER**

Determinations of whether Bank of America has failed to comply with this Consent Order, or any portion thereof, and whether to pursue any further action or relief against the Bank 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 Bank of America 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 Bank of America in this Consent Order and notwithstanding the releases and waivers herein. In the event FinCEN takes such action under this paragraph, the Bank 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 Bank of America'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 Bank of America as made a misrepresentation or failed to comply with this Consent Order, or any portion thereof, all statements made by or on behalf of the Bank 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. Bank of America 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 shall be treated as binding admissions, and Bank of America agrees that it shall 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 the Bank in determining whether Bank of America has violated any provision of this Consent Order.

## **XII. PUBLIC STATEMENTS**

Bank of America 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 Bank of America, or by any person under the authority, control, or speaking on behalf of Bank of America contradicts this Consent Order, and whether the Bank has repudiated such statement.

## **XIII. RECORD RETENTION**

In addition to any other record retention required under applicable law, Bank of America 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. Bank of America agrees to retain these records for a period of 6 years after creation of the record, unless required to retain them for a longer period of time under applicable law.

**XIV. SEVERABILITY**

Bank of America 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 Bank of America shall be construed and enforced accordingly.

**XV. SUCCESSORS AND ASSIGNS**

Bank of America agrees that the provisions of this Consent Order are binding on its owners, officers, employees, agents, representatives, affiliates, successors, assigns, and transferees to whom the Bank agrees to provide a copy of the executed Consent Order. Should Bank of America seek to sell, merge, transfer, or assign its operations, or any portion thereof, that are the subject of this Consent Order, the Bank 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.

**XVI. MODIFICATIONS AND HEADINGS**

This Consent Order can only be modified with the express written consent of FinCEN and Bank of America. 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.

**XVII. AUTHORIZED REPRESENTATIVE**

Bank of America'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 the Bank and further represents and warrants that Bank of America agrees to be bound by the terms and conditions of this Consent Order.

## **XVIII. 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 Bank of America:

Global General Counsel  
Bank of America, N.A.  
Bank of America Corporate Center  
100 North Tryon Street  
Charlotte, North Carolina 28255

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.

## **XIX. 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.

**XX. 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/ \_\_\_\_\_

Jenna Casanova  
Acting Director

Date:

Consented to and Approved By:

/s/ \_\_\_\_\_

Lauren Mogensen  
Global General Counsel  
Bank of America, N.A.

Date: