NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
ONE STATE STREET
NEW YORK, NEW YORK 10004

----------x

In the Matter of

PAXOS TRUST COMPANY, LLC

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and Paxos Trust Company, LLC ("Paxos" or the "Company") are willing to resolve the matters described herein without further proceedings.

WHEREAS, in 2015, the Department became the first financial regulator to establish a licensing and regulatory regime for virtual currency businesses and Paxos became the first company to secure a Limited Purpose Trust Charter for Digital Assets in New York;

WHEREAS, the Department's licensing regime and federal and New York laws require entities seeking to conduct virtual currency business in New York to, among other things, maintain effective controls for the purpose of guarding against money laundering and certain other illicit activities;

WHEREAS, in 2015, Paxos, formerly known as itBit Trust Company LLC, was granted a charter by the Department to operate as a limited purpose trust company, pursuant to Article III of the New York State Banking Law;

WHEREAS, in 2020, Paxos signed a letter agreement (the "2020 Letter Agreement") with the Department setting forth the terms and conditions that Paxos was expected to adopt and observe with respect to its ongoing relationship with Binance Holdings Limited ("Binance") and its administration of the Binance USD stablecoin;

WHEREAS, through an enforcement investigation, the Department found that Paxos failed to conduct proper due diligence of Binance as required by the 2020 Letter Agreement and that Paxos failed to maintain effective and compliant anti-money laundering and transaction monitoring programs; and

WHEREAS, Paxos has cooperated with the Department's investigation, has ended its relationship with Binance, and has undertaken comprehensive enhancements to its compliance function to prevent similar failures in the future.

NOW THEREFORE, in connection with an agreement to resolve this matter without further proceedings, pursuant to the Superintendent's authority under Sections 39 and 44 of the New York Banking Law, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

I. Parties and Regulatory Framework

A. The Parties

1. Paxos is a virtual currency company that offers various products and services, including stablecoins, asset tokenization services, settlement services, and cryptocurrency brokerage services. Paxos operates as a limited purpose trust company in New York under a charter granted by the Department in 2015.

2. The Department is the financial services regulator in the State of New York, and its head, the Superintendent of Financial Services (the "Superintendent"), bears the responsibility of ensuring the safety and soundness of New York's financial services industry and promoting the reduction and elimination of fraud, abuse, and unethical conduct with respect to financial institutions licensed to operate in the state.

3. The Department developed and oversees a first-of-its-kind regulatory framework pertaining to virtual currency businesses. Companies that conduct virtual currency business activity in the State of New York must be authorized to do so by the Department — either through the Department's Limited Purpose Trust Charter or through a BitLicense — and are subject to the Department's ongoing supervision.

4. Paxos, as a chartered limited purpose trust company authorized to conduct virtual currency business in New York State, is obligated to abide by the Department's laws and regulations. These regulations include establishing, implementing, and maintaining an effective anti-money laundering ("AML") program in addition to transaction monitoring and filtering programs.

5. The Superintendent has the power to conduct investigations, bring enforcement proceedings, levy monetary penalties, and order injunctive relief against parties who have violated relevant laws and regulations.

B. Anti-Money Laundering Regulations

6. Pursuant to 3 NYCRR § 116.2, Paxos is required to establish and maintain an effective and compliant AML program, including a robust customer due diligence program. This AML program should, at a minimum: (1) provide for a system of internal controls, policies, and procedures designed to ensure ongoing compliance with all applicable AML rules and

regulations; (2) provide for independent testing for compliance conducted by qualified internal personnel of the Department's licensee or a qualified external party; (3) designate a qualified individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (4) provide ongoing training for appropriate personnel.

C. Transaction Monitoring and Filtering Program Regulations

7. For bank and non-bank institutions, including Paxos, Part 504 of the Superintendent's Regulations establishes certain minimum requirements governing financial institutions' monitoring of customer transactions and compliance with United States Treasury Department's Office of Foreign Assets Control ("OFAC") screening requirements.

8. Specifically, Part 504.3(a) requires that each regulated institution shall maintain a transaction monitoring program reasonably designed for the purpose of monitoring transactions after their execution for potential Money Laundering/Terrorist Financing ("ML/TF") violations and suspicious activity reporting. The transaction monitoring program must be based on the risk assessment of the institution and be reviewed and periodically updated at risk-based intervals to take into account and reflect changes to applicable ML/TF laws, regulations, and regulatory warnings, as well as any other relevant information; appropriately match ML/TF risks to the institution's businesses; have ML/TF detection scenarios with threshold values and amounts designed to detect potential money laundering or other suspicious or illegal activities; have end-to-end, pre- and post-implementation testing; have documentation that articulates the institution's current detection scenarios and the underlying assumptions, parameters, and thresholds; have protocols setting forth how alerts generated by the Transaction Monitoring Program will be investigated, the process for deciding which alerts will result in a filing or other actions, the operating areas and individuals responsible for making such a decision, and how the

investigative and decision-making process will be documented; and be subject to an on-going analysis to assess the continued relevancy of the detection scenarios, the underlying rules, threshold values, parameters, and assumptions.

II. Events at Issue

A. Paxos's Compliance Failures Relating to Binance

i. Initial Due Diligence and Business Relationship with Binance

9. In September 2018, Paxos partnered with Binance, the world's largest digital asset exchange, to list its Paxos Standard ("PAX") stablecoin.

10. The following year, Paxos again partnered with Binance to market and distribute the Binance USD ("BUSD") stablecoin, with the intent to expand Paxos's market share and customer base beyond what it had previously achieved with PAX. In connection with this partnership, Paxos reviewed Binance's existing compliance program, including its AML policies and procedures and its geofencing controls. In July and August 2019, Paxos asked Binance to provide assurances that it had imposed geofencing controls to ensure that U.S. customers were not accessing an unregulated trading platform. Binance's Chief Compliance Officer responded, "[w]ith confidence, I can say the policies and procedures are already in effect" and later re-iterated that Binance.com was "completely restricting US persons." Paxos accepted Binance at its word and did not undertake an independent review of Binance's assertions or request supporting documentation beyond the initial review it had conducted on Binance for the listing of PAX.

11. Thereafter, the Department asked Paxos for information about Binance's compliance program. In response, Paxos collaborated with Binance and then drafted a letter for Binance to send to the Department, which it did in August 2019, stating: "Binance uses software

to detect user IP addresses and blocks those it determines are based in the U.S. In the event that a customer's IP is masked or a customer attempts to circumvent these IP restrictions (e.g., customer is using a Virtual Private Network), Binance employs a secondary manual control during the KYC process to check for U.S. persons and prevent onboarding." Binance's CCO approved the language in the letter, which was subsequently signed by Binance and submitted to the Department in August 2019. Paxos did not test or otherwise verify Binance's claims.

12. On July 24, 2020, Paxos signed the 2020 Letter Agreement with the Department that set forth the terms and conditions that Paxos was required to adopt and fulfill with respect to its ongoing relationship with Binance and the continued administration of BUSD.

13. Pursuant to the 2020 Letter Agreement, Paxos was obligated to review Binance's AML, sanctions, KYC, and related policies and procedures, and to maintain, administer, monitor, and revise effective controls to detect, prevent, and respond to any potential or actual wrongful use of BUSD. Paxos was further obligated to ensure that Binance timely informed Paxos of any material changes to those policies and procedures. The 2020 Letter Agreement further required Paxos to conduct periodic due diligence refreshes of Binance.

ii. Article About Binance's Geofencing Failures and Paxos's Response and Findings

14. In October 2020, a press outlet reported that Binance was accepting U.S. customers through the use of Virtual Private Networks ("VPNs") as a means to evade U.S. regulatory scrutiny. It further reported that Binance sought to undermine the ability of U.S. AML and sanctions enforcement to detect illicit activity occurring at or through Binance.

15. In response to the press report, the Department requested that Paxos provide information it had about the allegations. Paxos, in turn, requested information from Binance and

Binance confirmed that its U.S. restriction protocols remain unchanged. This time, however, Paxos requested that Binance support its assertion by, among other things, providing Paxos with Binance's independent AML audit and an audit focused specifically on Binance's geofencing controls. Binance provided its most recent KYC review report to Paxos and its CCO reiterated what Binance had told Paxos in the past, "as for our geo-fencing controls, you cannot even pass KYC if you are a U.S. person."

16. In fact, Binance's geofencing was deficient and circumventable by U.S. persons – a fact that Binance itself hinted at publicly. At least as early as April 2019, Binance published a guide on the "Binance Academy" section of its website, titled, "A Beginner's Guide to VPNs." The guide explained to customers that, "[i]f you want to be private about the websites you visit — and your location — you should use a VPN." Binance's VPN guide also stated: "you might want to use a VPN to unlock sites that are restricted in your country."

17. After the publication of the press report, Paxos began conducting monthly due diligence refreshes of Paxos transfers to Binance. In its first due diligence refresh, Paxos identified 99 U.S.-based Paxos retail and institutional clients who directly transferred BUSD from Paxos to Binance.com, including several large institutional trading firms and market makers based in the U.S. In addition, two of Paxos's employees with legacy Binance.com accounts tested Binance's supposed geographic restrictions. Both employees were able to access the exchange and make trades from New York IP addresses. Going forward, Paxos's monthly refresh routinely returned new and existing U.S. users transacting on Binance.com. Throughout the period of monthly refreshes, the number of U.S.-based Paxos users interacting with Binance.com generally declined each month and never exceeded the initial 99 accounts

identified. Paxos's refreshes and simple testing made clear, however, that even after the publication of the press report, Binance's supposed geofencing restrictions were, in fact, illusory.

iii. Binance's Exposure to Illicit Activity

18. Pursuant to the 2020 Letter Agreement, Paxos was required to conduct periodic risk assessments and due diligence refreshes of Binance and inform the Department immediately if there was a material increase in any risk involving or with respect to Binance.

19. Additionally, as a limited purpose trust company, Paxos is subject to supervisory examinations by the Department. Among other things, such examinations provide an opportunity for the Department to review a company's risk management and its Bank Secrecy Act ("BSA") /AML compliance program. In 2022, the Department concluded an examination of Paxos ("2022 Examination") and determined that Paxos failed to demonstrate that it had the appropriate controls in place to effectively monitor for significant illicit activity occurring at or through Binance and also failed to escalate red flags to Paxos's senior management and its Board.

20. The Department further noted in its October 2022 examination closing letter that, contrary to Paxos's position that, "Binance ha[d] a reasonable AML and Sanctions program in place," Binance had been significantly exposed to potentially illicit high-risk activity since shortly after Paxos entered into the 2020 Letter Agreement. The Department found that Paxos's knowledge of Binance's controls was based solely on a review of Binance's AML, sanctions, KYC, and related policies and procedures and the findings of Binance's external auditor's limited review of those same policies and procedures. Paxos did not have third-party assurances that attested to Binance's degree of compliance with its own policies and procedures.

21. As a result of the Department's 2022 Examination, which required Paxos to provide a report documenting Binance's exposure to sanctions, terrorist financing, darknet

marketplaces, and other illicit activity, Paxos requested that a third party blockchain analytics firm perform an enhanced due diligence ("EDD") investigation of Binance. The firm reviewed all historical Binance transactions from its founding in July 2017 to November 2022, across a select set of virtual currency assets. It identified $1.6 billion in transactions flowing to or from the Binance platform involving illicit actors including sanctioned individuals in darknet marketplaces and carding marketplaces and through Ponzi schemes. Additionally, the firm found that Binance had processed transactions to and from entities after OFAC had sanctioned them, including Chatex, Hydra Market, and Tornado Cash. For example, it found that Binance processed more than $32 million to or from Chatex, which had displayed Russian ransomware red flags, approximately $800,000 of which came after OFAC designated Chatex for facilitating financial transactions for ransomware actors.

22. Notwithstanding Paxos's representation to the Department that Binance had a reasonable AML and Sanctions program in place, in January 2023, Paxos's then Chief Compliance Officer wrote to the Company's Head of Corporate Strategy: "Binance appears to maintain a reasonable Compliance program, but Binance does not have an independent external audit report of their AML/Sanctions program which attests to the degree of compliance with its own policies and procedures, and the quality assurance reviews that were provided are incomplete and absent remediation plans."

23. On February 13, 2023, the Department announced that it had ordered Paxos to cease minting Paxos-issued BUSD as a result of unresolved issues related to the Company's oversight of its relationship with Binance. Paxos thereafter notified its customers of its intent to end its relationship with Binance for BUSD.

24. Paxos's failure to conduct proper due diligence of Binance with respect to its geofencing controls as well as its failure to conduct due diligence of Binance's deficient BSA/AML programs and policies constituted a breach of the 2020 Letter Agreement.

B. Paxos's Compliance Failures Unrelated to Binance

25. The BSA requires financial institutions to establish, implement, and maintain an effective AML program. New York law imposes these same requirements on regulated financial institutions such as Paxos.

26. The Department's investigation revealed that, prior to 2023, Paxos's BSA/AML compliance function was deficient. Notwithstanding the Department's guidance in 2022 to all virtual currency businesses highlighting the need to augment Know-your-Customer ("KYC")-related controls, Paxos onboarded customers with limited insight into their true identities, the legitimacy of their businesses, or the sources of their funds. As a result, customers who shared certain behavioral characteristics indicative of coordinated activity were able to open multiple accounts with Paxos. This program weakness was exacerbated by Paxos's lack of standardized investigation guidelines. In addition, though Paxos had written BSA/AML policies and procedures, they did not address certain trade-based money laundering risks; nor did Paxos specifically train its compliance staff to identify those risks. These failures created an environment vulnerable to exploitation by criminal actors.

i. Paxos's Know-your-Customer Failures

27. A core component of an effective BSA/AML program is an institution's KYC program. A successful KYC program enables financial institutions to establish the identity of a person or entity, assign a risk rating to the customer, and then effectively manage the risk. This first line of defense is critical to combating financial crime.

28. To manage its KYC program, Paxos's compliance staff used a centralized software tool to review its customers' information, including KYC and transactional activity, and to take action, including processing user onboardings and assigning customer risk ratings. Paxos's software, however, did not include automated alerts to indicate potentially risky shared customer attributes or provide frontline search capabilities during the onboarding process. This weakness enabled customers who shared addresses, corporate documents, beneficial owners, and certain behavioral characteristics indicative of potential illicit coordinated activity to open multiple accounts and remain undetected.

29. For example, Paxos onboarded 11 businesses located in the same single-story strip mall in South Florida without identifying their shared attributes and Paxos's deficient compliance user interface did not generate an alert. Compliance staff at Paxos acknowledged that the system did not adequately address the "linking" of individuals and entities. Three of these businesses were associated with an individual who had transacted approximately $260 million on the exchange during a period of fourteen months. This individual was listed as the accountant for a company that prepared the corporate books for at least four other customers onboarded to the platform.

30. Financial institutions can guard against money laundering by requiring verification of a prospective customer's source of funds. Although Paxos's written policies required that customers provide information on their source of funds, occupation, and a stated purpose for the account and business relationship, Paxos failed to take reasonable steps to investigate account holders who submitted suspicious account opening or EDD materials. Paxos employees, instead, relied on prospective customers' written responses during the EDD process and did not obtain adequate supporting documentation. When questioned by Paxos employees

about their businesses, customers were able to submit unverified photographs and provide other generalized answers to pass Paxos's EDD requirements. Customers were also able to onboard with false or insufficient documentation (e.g., invoices and bank statements) that did not align with the entity's stated business activity or purpose.

31. In 2023, Paxos's employees commented on Paxos's lax approach toward customer due diligence. For example, one Paxos compliance employee wrote, "I feel like every export or trading company we have on platform is fake[.]" Another compliance employee noted, "so they told us they are an unlicensed [money services business] . . . and we onboarded [laughing out loud] . . . also they are an [over-the-counter] desk . . . zero trades." A third compliance employee's comment is illustrative of Paxos's significant EDD failings: "Yea, going through this newer one I found, we never received anything from them showing that they should be conducting this volume of activity. Just a bunch of likely fake policies and org docs and then just let them go because they are an [over-the-counter] desk[.]"

32. In 2023, a third-party auditor, engaged to audit the company from July 2021 through June 2022, identified deficiencies in the company's customer due diligence process at onboarding and thereafter cautioned that such gaps could result in inaccurate identification and inaccurate assessment of the customers' money laundering risk.

ii. Paxos's Transaction Monitoring Failures

33. As discussed above, maintaining an effective transaction monitoring and filtering program is an important component of a financial institution's BSA/AML framework. The Department's investigation revealed Paxos's failures in this area as well.

34. To avoid raising alerts within banking and money transmitter systems, money launderers often break up large transactions into smaller transactions. To anonymize the

transactions, money launderers often use multiple real or fabricated identities on either side of the transaction. A compliant AML program will include control scenarios to detect attempts to structure transactions.

35. In 2019, 2020, and 2021, Paxos's risk assessments rated the Company's transaction monitoring capabilities as "fair" due to the retrospective nature of the systems. As the Company's then BSA Officer explained in March of 2020, ". . . [F]or AML if there were a potential pattern of transactions indicative of money laundering or [Bitcoin] sourced from a darknet marketplace, we would not know until 2-4 weeks later." Paxos's manually intensive and technologically limited processes to monitor withdrawals in real-time prevented it from detecting obvious and easily detectable patterns of money laundering. Paxos's quality assurance team found as much, noting that Paxos failed to identify certain alerts as potentially suspicious and thus warranting an investigation.

36. Such was the case with a network of customers who engaged in a trade-based money laundering scheme (the "TBML network") on Paxos's exchange for approximately five years. Their transactions followed one of two patterns: (l) a rapid movement of funds from fiat to cryptocurrency or (2) a rapid movement of funds from cryptocurrency deposit to fiat (specifically U.S. dollar wire withdrawal of all funds off the platform to U.S.-based financial institutions). Some transactions occurred within minutes of each other, many deposits were in round-dollar amounts, and the customers rarely, if ever, maintained a balance on the Paxos platform. Based on the rapid movement of high-volume transactions, the use of multiple accounts, and small to zero end-of-day balances, it is likely that the accounts were used to layer funds, a means of money launderers to avoid detection of the actual source of the funds. Although many of these customers onboarded to the Paxos platform with the stated intention of

buying and selling cryptocurrency, their transactions on the platform indicated otherwise and these suspicious transactions went undetected.

37. By 2022, although Paxos had made improvements to its transaction monitoring systems, it was still failing to appropriately tune these systems to the relevant AML risks by performing assessments on the business rules and scenarios employed by the systems. That same year, the Department issued industry guidance regarding Blockchain analytics and emphasized the importance of appropriately tailoring monitoring programs.

iii. Paxos's Investigations Failures

38. While transaction monitoring and the detection of suspicious patterns are vital components of an effective AML program, the obligations of Department licensees do not end there. Licensees must maintain protocols that set forth how alerts generated by their transaction monitoring programs will be investigated, the process for deciding which alerts will result in a filing or other action, the operating areas and individuals responsible for making such a decision, and how the investigative and the decision-making process will be documented.

39. Prior to 2022, Paxos's formal investigations policy did not require an investigation upon receipt of a law enforcement request, and instead left the decision of whether to perform an investigation to the discretion of the investigator. Thus, even if the pattern of transactions described in connection with the TBML network had resulted in alerts, it is unclear what, if any, investigation would have followed. Paxos was on notice of this failing. A 2021 audit of its BSA/AML program included a finding that for SAR filing procedures, there were insufficient details for minimum due diligence required for case investigations. In 2022, Paxos's internal audit also identified this as an outstanding issue, noting that the Company lacked defined case investigation procedures to comprehensively describe the minimum requirements for

investigative research and due diligence. After the TBML network had been discovered, this finding was repeated in a 2023 audit covering 2022 activity. That audit noted that Paxos's case investigation procedures did not include minimum requirements for performing and documenting investigative research and due diligence. An external consulting firm hired by Paxos after the discovery of the TBML network found that the Company failed to investigate 79 of 188 information requests it received in a two-year period. In early 2023, the relevant policy was updated to require investigation following receipt of a law enforcement request.

40. An example of the failure of Paxos to conduct thorough investigations was the TBML network. Of this network of customers, 32 accounts had previously been brought to Paxos's attention through law enforcement subpoenas or information requests from other financial institutions. Notwithstanding these inquiries, Paxos's compliance staff failed to identify the larger network. Paxos's quality assurance team reported that team members indicated that they did not want or did not have the time to investigate alerts. The quality assurance team also found that there was a lack of accountability for poor quality work by Paxos employees.

41. In light of these compliance and due diligence failures, enforcement action is warranted, including a monetary penalty.

Cooperation

42. Paxos complied with the Department's order that it cease minting Paxos-issued BUSD and cooperated in connection with the termination of its relationship with Binance.

43. The Department has given substantial weight to the cooperation of Paxos both in the course of the enforcement investigation and in connection with the Department's oversight of Paxos's termination of its relationship with Binance.

44. Additionally, the Department recognizes Paxos's efforts to improve and strengthen its compliance function, including by growing its compliance team, expanding the scope of its vendor support and expertise, and dedicating personnel from outside of its compliance division to develop compliance tooling. Paxos also engaged an outside consultant upon learning of AML program deficiencies in January 2023. As part of that engagement, the consulting company conducted a broad multi-year lookback and root cause analysis, the results of which Paxos shared with the Department in periodic updates and a final report. Paxos worked with the consultant to implement recommended remediation steps in real-time during the engagement.

Violations of Law and Regulations

45. Paxos failed to maintain an effective and compliant AML program, in violation of 3 NYCRR § 116.2.

46. Paxos conducted business in an unsafe and unsound manner, in violation of New York Banking Law § 44.

47. Paxos breached the 2020 Letter Agreement, in violation of New York Banking Law § 44.

48. Paxos failed to comply with its obligations to maintain an effective transaction monitoring program, in violation of 23 NYCRR § 504.3.

NOW THEREFORE, to resolve this matter without further proceedings, the Department and the Company stipulate and agree to the following terms and conditions:

SETTLEMENT PROVISIONS

Monetary Penalty

49. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, Paxos shall pay a total civil monetary penalty pursuant to Banking Law §§ 39

and 44 to the Department in the amount of twenty-six million and five hundred thousand dollars and 00/100 Cents ($26,500,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

50. The Company shall not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

51. The Company shall neither seek nor accept, directly or indirectly, reimbursement or indemnification with respect to payment of the penalty amount, including but not limited to, payment made pursuant to any insurance policy.

Remediation and Compliance

52. In addition to the civil monetary penalty set forth above, Paxos shall commit, at a minimum, twenty-two million dollars and 00/100 Cents ($22,000,000.00) to continue to improve and strengthen its compliance function over the years 2025 through 2027. As of the date of this Consent Order, Paxos has already spent $3,100,000 for the year 2025 in connection with improving and operating its compliance program.

53. Paxos shall set aside $3,150,000 in connection with its compliance program to be spent over the remainder of the year 2025. No later than January 1, 2026, Paxos shall specifically set aside $7,250,000 to be spent in 2026 in connection with its compliance program. No later than January 1, 2027, Paxos shall specifically set aside $8,500,000 to be spent in 2027 in connection with its compliance program.

54. Within thirty (30) days of Paxos's commitment of the dollar amounts listed above in paragraph 53 to be set aside in connection with Paxos's expenditure to improving and

operating its compliance program, Paxos shall submit to the Department written confirmation that it has set aside such funds.

Status Report

55. Within ninety (90) days of the execution of this Consent Order, the Company shall submit a Status Report (hereinafter the "Status Report") acceptable to the Department on the following:

Customer Due Diligence

56. Regarding customer due diligence, the Status Report shall include updates on, at a minimum, the Company's:

a. policies, procedures, and controls to ensure that the Company collects, analyzes, and retains complete and accurate customer information for all account holders;

b. methodology and plans for subsequent enhancements for assigning risk ratings to account holders that considers additional factors such as type of customer, type of products and services, geographic location(s), and transaction volume;

c. methodology to evaluate customers whose transactional activity requires additional enhanced due diligence and procedures to:

   i. determine the additional documentation necessary to verify the identity and business activities of the customer;

   ii. evaluate anticipated activity versus actual transaction activity of the customer;

d. enhancements to the periodic review process for the entire customer base to ensure that all necessary customer and account information is up to date;

e. the customer risk rating system, including the Company's policies and procedures governing the system; and

f. the status of any vendor integration in connection with the customer due diligence process.

BSA/AML Compliance Program

57. Regarding BSA/AML compliance, the Status Report shall include updates on, at a minimum:

a. Paxos's current system of internal controls reasonably designed to ensure compliance with BSA/AML requirements and relevant state laws and regulations;

b. Paxos's most recent annual comprehensive BSA/AML risk assessment that identifies and considers all of the Company's products and services, customer types, geographic locations, and transaction volumes, as appropriate, in determining inherent and residual risks;

c. the management of the Company's BSA/AML compliance program by a qualified compliance officer, who is given autonomy, independence, and responsibility for implementing and maintaining an effective BSA/AML compliance program that is commensurate with the Company's size and risk profile, and is supported by adequate staffing levels and resources;

d. the case management systems on which Paxos can reasonably rely to ensure compliance with BSA/AML requirements and relevant state laws and regulations, and a timeline to review key systems to ensure that the case management systems are configured to mitigate BSA/AML risks;

e. the comprehensive and timely independent testing of the Company's compliance with applicable BSA/AML requirements and relevant state laws and regulations;

f. the effective training of all appropriate personnel at the Company who perform BSA/AML compliance-related functions in all aspects of BSA/AML requirements, relevant state laws and regulations, and relevant internal policies and procedures; and

g. enhancements to Paxos's case management system, including comprehensive metric reporting, ability to include key risk indicators, and product and customer segmentation.

Suspicious Activity Monitoring and Reporting

58. Regarding suspicious activity monitoring and reporting, the Status Report shall include updates on, at a minimum, the Company's improvement and operation of:

a. a system of internal controls reasonably designed to conduct ongoing transaction monitoring to ensure compliance with suspicious activity

regulatory reporting requirements, including the effective monitoring of customer accounts and the maintenance of accurate and comprehensive transactional data;

b. a well-documented methodology for establishing monitoring rules and thresholds appropriate for Paxos, considering factors such as type of customer, type of product or service, and geographic location;

c. policies and procedures for analyzing, testing, and documenting changes to the Company's monitoring rules and thresholds; and

d. enhanced investigation and reporting criteria and procedures to ensure the timely detection, investigation, and reporting of all known or suspected violations of law and suspicious transactions, including, but not limited to:

i. the appropriate allocation of resources to manage suspicious activity alert and case inventory;

ii. policies and/or procedures of the Company's investigation and analysis of potentially suspicious activity, including its escalation and review of concerns through appropriate levels of management.

Corporate Governance, Management Oversight and Reporting

59. Regarding corporate governance, management oversight, and reporting, the Status Report shall include updates on, at a minimum:

a. actions that the Company has taken and will take to maintain effective control over and oversight of compliance with BSA/AML requirements and relevant state laws and regulations;

b. actions that the Company has taken and will take to improve its reporting to senior management about the Company's compliance with BSA/AML requirements and state laws and regulations;

c. the current status of clearly defined roles, responsibilities, and accountability for the Company's respective management, compliance personnel, and independent audit staff regarding compliance with BSA/AML requirements and state laws and regulations;

d. measures that Paxos has taken and will take to ensure that the Company's senior management appropriately track, escalate, and review BSA/AML compliance concerns;

e. measures that the Company has taken and will take to ensure that the person or groups at the Company charged with the responsibility of overseeing the Company's compliance with BSA/AML requirements and

relevant state laws and regulations possess appropriate subject matter expertise and are actively involved in carrying out such responsibilities; the Company's expenditure of adequate resources to ensure its compliance with this Order, BSA/AML requirements, and state laws and regulations; and

f. actions that the Company has taken and will take to establish an appropriate and effective reporting structure that permits the Company's BSA/AML compliance officer to report information in a timely and complete manner to relevant Company personnel, including the Company's senior management.

Case and Rules Management

60. Regarding case and rules management, the Status Report shall include updates on, at a minimum, the Company's:

a. further enhancements to its current case management system;

b. integration of advanced analytics into Paxos's administration platform;

c. centralized process, and enhancements thereto, for managing rule logic and system configurations used in case and rules management, ensuring alignment with documented policy requirements and model governance standards; and

d. structured framework, and enhancements thereto, for rule change management controls and maintenance of comprehensive audit trail capabilities.

Technical Program Support

61. Regarding technical program support, the Status Report shall include updates on, at a minimum:

a. the development and maintenance of platform operations in connection with incident response processes;

b. updates on the Company's technical support capabilities; and

c. updates on enhancements to ensure continuous compliance effectiveness and system stability.

62. Every six months from the Effective Date of this Consent Order (as defined below), for a period of three years from the Effective Date, Paxos shall submit to the Department

written progress reports detailing the form, manner, and anticipated completion date of all actions taken to secure compliance with the provisions of this Order and the results thereof, including, but not limited to, the steps enumerated in paragraphs 56 to 61 above. This reporting obligation may be extended by the Department, in its sole regulatory discretion, by providing written notice to the Company.

Full and Complete Cooperation

63. Paxos commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order.

Further Action by the Department

64. No further action will be taken by the Department against the Company or its successors for the conduct set forth in this Consent Order, provided that the Company fully complies with the terms of the Consent Order.

65. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against the Company for transactions or conduct that were not disclosed in the written materials submitted to the Department in connection with this matter.

Waiver of Rights

66. The Company submits to the authority of the Superintendent to effectuate this Consent Order.

67. The parties understand and agree that no provision of this Consent Order is subject to review in any court, tribunal, or agency outside of the Department.

Parties Bound by the Consent Order

68. This Consent Order is binding on the Department and the Company, as well as any successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

Breach of Consent Order

69. In the event that the Department believes the Company to be in material breach of the Consent Order, the Department will provide written notice to the Company, and the Company must, within ten (10) days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

70. The Company understands and agrees that its failure to make the required showing within the designated time period shall be presumptive evidence of the Company's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all the remedies available to it under New York Banking Law and New York Financial Services Law, and any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

71. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Joseph C. Mineo
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One Commerce Plaza
Albany, New York 12257

For Paxos Trust Company LLC:

Leighton Dellinger
Head of Legal
Paxos Trust Company, LLC
450 Lexington Ave,
New York, New York 10163

Laurel Loomis Rimon
Jenner & Block LLP
1099 New York Ave., NW
Washington, DC 20001

Miscellaneous

72. This Consent Order and any dispute thereunder shall be governed by the laws of the State of New York without regard to any conflicts of laws principles.

73. This Consent Order may not be altered, modified, or changed unless in writing and signed by the parties hereto.

74. This Consent Order constitutes the entire agreement between the Department and the Company and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order.

75. Each provision of this Consent Order shall remain effective and enforceable against the Company, its successors, and assigns, until stayed, modified, suspended, or terminated by the Department.

76. In the event that one or more provisions contained in this Consent Order shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

77. No promise, assurance, representation, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of this Consent Order.

78. Nothing in this Consent Order shall be construed to prevent any consumer or any other third party from pursuing any right or remedy at law.

79. This Consent Order may be executed in one or more counterparts and shall become effective when such counterparts have been signed by each of the parties hereto (the "Effective Date").

[remainder of this page intentionally left blank]

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s/ Kathryn A. Taylor
KATHRYN A. TAYLOR
Deputy Director of Enforcement for Consumer Protection and Financial Enforcement

August 4, 2025

By: /s/ Christopher B. Mulvihill
CHRISTOPHER B. MULVIHILL
Deputy Superintendent for Consumer Protection and Financial Enforcement

August 4, 2025

By: /s/ R. Gabriel D. O'Malley
R. GABRIEL D. O'MALLEY
Executive Deputy Superintendent for Consumer Protection and Financial Enforcement

August 4, 2025

PAXOS TRUST COMPANY, LLC

By: /s/ Charles G. Cascarilla
CHARLES G. CASCARILLA
Chief Executive Officer

August 1, 2025

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services

August 7, 2025