UNITED STATES OF AMERICA
DEPARTMENT OF THE TREASURY
OFFICE OF THE COMPTROLLER OF THE CURRENCY

In the Matter of:	)	
	)	
Capital One, N.A. Mclean, Virginia	)	AA-EC-20-49
	)	
Capital One Bank (USA), N.A. Glen Allen, Virginia	)	
	)	

CONSENT ORDER

WHEREAS, the Office of the Comptroller of the Currency ("OCC") has supervisory authority over Capital One, N.A., McLean, Virginia and Capital One Bank (USA), N.A., Glen Allen, Virginia (collectively, the "Bank");

WHEREAS, the OCC intends to initiate cease and desist proceedings against the Bank pursuant to 12 U.S.C. § 1818(b), through the issuance of a Notice of Charges, for engaging in unsafe or unsound practices, including those relating to information security, and noncompliance with 12 C.F.R. Part 30;

WHEREAS, in the interest of cooperation and to avoid additional costs associated with administrative and judicial proceedings with respect to the above matter, the Bank, by and through its duly elected and acting Board of Directors ("Board"), consents to the issuance of this Consent Order ("Order"), by the OCC through the duly authorized representative of the Comptroller of the Currency ("Comptroller"); and

NOW, THEREFORE, pursuant to the authority vested in the OCC by Section 8(b) of the Federal Deposit Insurance Act, as amended, 12 U.S.C. § 1818(b), the OCC hereby orders that:

ARTICLE I

JURISDICTION

(1) The Bank is an "insured depository institution" as that term is defined in 12 U.S.C. § 1813(c)(2).

(2) The Bank is a national banking association within the meaning of 12 U.S.C. § 1813(q)(1)(A), and is chartered and examined by the OCC. *See* 12 U.S.C. § 1 *et seq.*

(3) The OCC is the "appropriate Federal banking agency" as that term is defined in 12 U.S.C. § 1813(q) and is therefore authorized to initiate and maintain this cease and desist action against the Bank pursuant to 12 U.S.C. § 1818(b).

ARTICLE II

COMPTROLLER'S FINDINGS

The Comptroller finds, and the Bank neither admits nor denies, the following:

(1) In or around 2015, the Bank failed to establish effective risk assessment processes prior to migrating its information technology operations to the cloud operating environment. The Bank also failed to establish appropriate risk management for the cloud operating environment, including appropriate design and implementation of certain network security controls, adequate data loss prevention controls, and effective dispositioning of alerts.

(2) The Bank's internal audit failed to identify numerous control weaknesses and gaps in the cloud operating environment. Internal audit also did not effectively report on and highlight identified weaknesses and gaps to the Audit Committee.

(3) For certain concerns raised by internal audit, the Board failed to take effective actions to hold management accountable, particularly in addressing concerns regarding certain internal control gaps and weaknesses.

(4) By reason of the foregoing conduct, the Bank was in noncompliance with 12 C.F.R. Part 30, Appendix B, "Interagency Guidelines Establishing Information Security Standards," and engaged in unsafe or unsound practices that were part of a pattern of misconduct.

(5) The Bank has begun addressing the identified corrective action and has committed to providing resources to remedy the deficiencies.

ARTICLE III

COMPLIANCE COMMITTEE

(1) By August 31, 2020, the Board shall appoint a Compliance Committee of at least three (3) members of which a majority shall be directors who are not employees or officers of the Bank or any of its subsidiaries or affiliates. The Board shall submit in writing to the Examiner-in-Charge the names of the members of the Compliance Committee within ten (10) days of their appointment. In the event of a change of the membership, the Board shall submit in writing to the Examiner-in-Charge within ten (10) days the name of any new or resigning committee member. The Compliance Committee shall monitor and oversee the Bank's compliance with the provisions of this Order. The Compliance Committee shall meet at least quarterly and maintain minutes of its meetings.

(2) By October 30, 2020, and thereafter within forty-five (45) days after the end of each quarter, the Compliance Committee shall submit to the Board a written progress report setting forth in detail:

(a) A description of the corrective actions needed to achieve compliance with each Article of this Order;

(b) The specific corrective actions undertaken to comply with each Article of this Order; and

(c) The results and status of the corrective actions.

(3) Upon receiving each written progress report, the Board shall forward a copy of the report, with any additional comments by the Board, to the Examiner-in-Charge within ten (10) days of the first Board meeting following the Board's receipt of such report.

ARTICLE IV

COMPREHENSIVE ACTION PLAN

(1) Within sixty (60) days of the effective date of this Order, the Bank shall develop a written action plan detailing the remedial actions necessary to achieve compliance with Articles V through X of this Order ("Action Plan"), and submit the Action Plan to the Examiner-in-Charge for review and prior written determination of no supervisory objection by the Deputy Comptroller. To the extent the remedial actions and action plans identified in Articles V through X are already addressed in the Bank's four previously adopted actions plans ("Existing Bank Action Plans"), the Existing Bank Action Plans may be used to satisfy the Action Plan and action plans required in Articles V through X. The Action Plan, at a minimum, shall specify:

(a) A description of the corrective actions needed to achieve compliance with each Article of this Order;

(b) Reasonable and well-supported timelines for completion of the corrective actions required by this Order; and

(c) The person(s) responsible for completion of the corrective actions required by this Order.

(2) The timelines contained in the Action Plan shall be consistent with any deadlines set forth in this Order, including any modifications to the Order made pursuant to Article XIV, Paragraph (4).

(3) In the event the Deputy Comptroller requires changes to the Action Plan, the Bank shall incorporate the required changes into the Action Plan and submit the revised Action Plan to the Examiner-in-Charge for review and prior written determination of no supervisory objection by the Deputy Comptroller.

(4) Upon receipt of a written determination of no supervisory objection from the Deputy Comptroller, the Board shall ensure the Bank has timely adopted and implemented all corrective actions required by this Order, and shall verify the Bank adheres to the Action Plan, including the timelines set forth within the Action Plan.

(5) The Bank shall not take any action that will cause a significant deviation from, or material change to, the Action Plan. Where the Bank considers modifications to the Action Plan appropriate, the Bank shall submit a revised Action Plan containing the proposed modifications to the Examiner-in-Charge for prior written determination of no supervisory objection from the Deputy Comptroller. Upon receipt of a written determination of no supervisory objection from the Deputy Comptroller, the Board shall ensure the Bank has timely adopted and implemented all corrective actions required by this Order, and shall verify the Bank adheres to the revised Action Plan.

(6) By October 30, 2020, and thereafter within forty-five (45) days after the end of each quarter, the Bank shall prepare, and shall submit to the Board, a written Action Plan progress report setting forth in detail:

(a) The specific corrective actions undertaken to comply with each Article of this Order;

(b) The results and status of the corrective actions; and

(c) A description of the outstanding corrective actions needed to achieve compliance with each Article of this Order and the party or parties responsible for the completion of outstanding corrective actions.

The Board shall direct the Bank to forward a copy of the report, with any additional comments by the Board, to the appropriate OCC official within ten (10) days of the first Board meeting following the Board's receipt of such report.

ARTICLE V

BOARD AND MANAGEMENT OVERSIGHT

(1) Within ninety (90) days of the effective date of this Order, the Bank shall submit to the OCC, for review and prior written determination of no supervisory objection by the Examiner-in-Charge, a plan to improve oversight of the Bank's cloud operating environment information security program ("Board and Management Oversight Plan"). At a minimum, the Board and Management Oversight Plan shall require the Bank to:

(a) Develop appropriate and effective risk assessment processes across all three lines of defense to identify and manage technology risks within the cloud operating environment, including risk assessment processes specific to technology changes;

(b) Reassess the quality and content of Board reporting and improve transparency into the materiality and status of known technology and cyber risk issues;

(c) Increase scrutiny, monitoring, and oversight of management's actions to address significant technology and cyber risk issues, including audit findings; and

(d) Hold management accountable for the timely remediation of material risk issues identified by internal and external sources, including requiring management to explain why key issues and risks related to the cloud operating environment have not been addressed in a timely and effective manner.

ARTICLE VI

RISK ASSESSMENT

(1) Within ninety (90) days of the effective date of this Order, the Bank shall develop and submit to the OCC, for review and prior written determination of no supervisory objection by the Examiner-in-Charge, a plan to improve risk assessment for the Bank's cloud and legacy technology operating environments ("Risk Assessment Plan"). At a minimum, the Risk Assessment Plan shall require the Bank to:

(a) Document expected and potential threats of material changes to the cloud and legacy technology environments and mitigating controls or remediation plans to address such threats;

(b) Develop appropriate risk mitigation testing from the beginning and throughout new project life cycle;

(c) Create a current threat inventory for use in risk assessment processes;

(d) Maintain the current threat inventory through continuous updating and analyzing of information regarding new threats and vulnerabilities, actual attacks, and the effectiveness of existing security controls; and

(e) Reassess critical business processes related to cyber and technology change activity to ensure they are appropriately captured and included in existing risk assessment processes.

(2) The Risk Assessment Plan shall expand existing risk assessment processes and supporting policies and procedures to include coverage and guidance on the criteria against which to perform targeted risk assessments of material cyber and technology change initiatives.

(3) The Risk Assessment Plan shall redesign the enterprise risk assessment framework to capture and aggregate results of all relevant risk identification and control effectiveness inputs to drive enterprise risk reporting of cyber and technology change risk.

(4) The Bank shall not implement a material technology or cyber change initiative before development and submission of a comprehensive risk assessment for the change initiative to the Examiner-in-Charge. This requirement is effective upon submission of the Bank's Risk Assessment Plan as detailed in this Article.

ARTICLE VII

CLOUD OPERATIONS RISK MANAGEMENT

(1) Within ninety (90) days of the effective date of this Order, the Bank shall submit to the OCC, for review and prior written determination of no supervisory objection by the Examiner-in-Charge, a plan to improve the Bank's Cloud Operations Risk Management ("Cloud Operations Risk Management Plan"). At a minimum, the Cloud Operations Risk Management Plan shall require the Bank to implement effective corrective actions required as a result of a

2019 OCC examination. The Cloud Operations Risk Management plan shall broadly require the Bank to:

(a) Develop comprehensive security controls protecting the Bank's network perimeter;

(b) Develop effective controls to identify and protect sensitive customer information contained within the Bank's technology systems and applications;

(c) Develop comprehensive processes to prevent and detect unauthorized disclosure of sensitive information sent outside the Bank's technology environment; and

(d) Develop effective vulnerability and configuration management controls related to the containerization of objects within the Bank's cloud environment.

ARTICLE VIII

INDEPENDENT RISK MANAGEMENT

(1) Within ninety (90) days of the effective date of this Order, the Bank shall submit to the OCC, for review and prior written determination of no supervisory objection by the Examiner-in-Charge, a plan to improve independent risk management of the cloud operating environment ("Independent Risk Management Plan"). At a minimum, the Independent Risk Management Plan shall require the Bank to:

(a) Assess inherent technology and cyber risks enterprise-wide and deploy appropriate and effective controls to mitigate these risks;

(b) Challenge inherent and residual cyber risks as identified by technology and cyber first line functions;

(c) Formally define and document a comprehensive cyber risk and control universe that captures all relevant risks; and

(d) Utilize control universe data to create and implement an appropriate risk-based control testing and validation plan.

ARTICLE IX

INTERNAL CONTROLS TESTING

(1) Within ninety (90) days of the effective date of this Order, the Bank shall submit to the OCC, for review and prior written determination of no supervisory objection by the Examiner-in-Charge, a plan designed to enhance the Bank's internal controls testing in the cloud environment ("Internal Controls Plan"). At a minimum, the Internal Controls Plan shall require the Bank to:

(a) Develop a control inventory by identifying and documenting relevant controls within the Bank's cloud operating environment;

(b) Develop and implement a comprehensive risk-based testing and monitoring plan that is reconciled back to the inventory; and

(c) Track and remediate control gaps, or appropriately approve control gaps as a risk acceptance.

ARTICLE X

INTERNAL AUDIT

(1) Within ninety (90) days of the effective date of this Order, the Bank shall submit to the Examiner-in-Charge for review and prior written determination of no supervisory

objection a plan to enhance the Bank's internal audit program ("Internal Audit Plan"). At a minimum, the Internal Audit Plan shall require the Bank to:

(a) Reassess the cyber and technology risk assessment methodology and scoring system that ranks and evaluates business and control risks for significant business units, products, services, and security functions;

(b) Assess and validate the completeness and accuracy of management's documented inventory of technology assets and configurable devices and software;

(c) Map the existing audit universe to the concerns noted in the recent examination to identify coverage gaps and audit quality issues;

(d) Incorporate lessons-learned related to the cybersecurity breach root cause analysis;

(e) Revise the risk-based technology audit plan to address the gaps and weaknesses described in Article II and within audit's lessons-learned assessment to ensure appropriate coverage of cloud operations and related security controls; and

(f) Assess audit staff expertise and training needs.

(2) The Internal Audit Plan shall also include improved reporting to the Audit Committee to appropriately capture detailed technology risk issues and control themes and ineffective or untimely remediation efforts to provide the Board with sufficient information to make informed decisions regarding risks within the IT operating and control environment.

ARTICLE XI

GENERAL BOARD RESPONSIBILITIES

(1) The Board shall ensure that the Bank has timely adopted and implemented all corrective actions required by this Order, and shall verify that the Bank adheres to the corrective actions and they are effective in addressing the Bank's deficiencies that resulted in this Order.

(2) In each instance in which this Order imposes responsibilities upon the Board, it is intended to mean that the Board shall:

(a) Authorize, direct, and adopt corrective actions on behalf of the Bank as may be necessary to perform the obligations and undertakings imposed on the Board by this Order;

(b) Ensure the Bank has sufficient processes, management, personnel, control systems, and corporate and risk governance to implement and adhere to all provisions of this Order;

(c) Require that Bank management and personnel have sufficient training and authority to execute their duties and responsibilities pertaining to or resulting from this Order;

(d) Hold Bank management and personnel accountable for executing their duties and responsibilities pertaining to or resulting from this Order;

(e) Require appropriate, adequate, and timely reporting to the Board by Bank management of corrective actions directed by the Board to be taken under the terms of this Order; and

(f) Address any noncompliance with corrective actions in a timely and appropriate manner.

ARTICLE XII

WAIVERS

(1) The Bank, by executing and consenting to this Order, waives:

(a) Any and all rights to the issuance of a Notice of Charges pursuant to 12 U.S.C. § 1818;

(b) Any and all procedural rights available in connection with the issuance of this Order;

(c) Any and all rights to a hearing and a final agency decision pursuant to 12 U.S.C. § 1818 and 12 C.F.R. Part 19;

(d) Any and all rights to seek any type of administrative or judicial review of this Order;

(e) Any and all claims for fees, costs, or expenses against the OCC, or any of its officers, employees, or agents related in any way to this enforcement matter or this Order, whether arising under common law or under the terms of any statute, including, but not limited to, the Equal Access to Justice Act, 5 U.S.C. § 504 and 28 U.S.C. § 2412;

(f) Any and all rights to assert this proceeding, the consent to and/or the issuance of this Order, as the basis for a claim of double jeopardy in any pending or future proceeding brought by the United States Department of Justice or any other governmental entity; and

(g) Any and all rights to challenge or contest the validity of this Order.

ARTICLE XIII

OTHER PROVISIONS

(1) Regarding the effect of this Order, and unless the OCC informs the Bank otherwise in writing with respect to any or all of the subparts below:

(a) Pursuant to 12 C.F.R. § 5.3(g)(5), the Bank may be treated as an eligible bank for the purposes of 12 C.F.R. Part 5, subject to the requirements contained in 12 C.F.R. § 5.3(g)(1)-(4);

(b) Pursuant to 12 C.F.R. § 5.51(c)(7)(ii), the Bank is not subject to the restrictions in 12 C.F.R. § 5.51 requiring prior notice to the OCC of changes in directors and senior executive officers or the limitations on golden parachute payments set forth in 12 C.F.R. Part 359, subject to the requirements contained in 12 C.F.R. § 5.51(c)(7)(i), (iii); and

(c) Pursuant to 12 C.F.R. § 24.2(e)(4), the Bank may be treated as an "eligible bank" for the purposes of 12 C.F.R. Part 24, subject to the requirements contained in 12 C.F.R. § 24(e)(1)-(3).

(2) This Order supersedes all prior OCC communications issued pursuant to 12 C.F.R. §§ 5.3(g)(5), 5.51(c)(7)(ii), and 24.2(e)(4).

ARTICLE XIV

CLOSING

(1) This Order is a settlement of the cease and desist proceeding against the Bank contemplated by the OCC, based on the unsafe or unsound practices and violations of regulation described in the Comptroller's Findings set forth in Article II of this Order. The OCC releases and discharges the Bank from all potential liability for a cease and desist order that has been or

might have been asserted by the OCC based on the practices and violations described in Article II of this Order, to the extent known to the OCC as of the effective date of this Order. Nothing in this Order, however, shall prevent the OCC from:

(a) Instituting enforcement actions other than a cease and desist order against the Bank based on the Comptroller's Findings set forth in Article II of this Order;

(b) Instituting enforcement actions against the Bank based on any other findings;

(c) Instituting enforcement actions against institution-affiliated parties (as defined by 12 U.S.C. § 1813(u)) based on the Comptroller's Findings set forth in Article II of this Order, or any other findings; or

(d) Utilizing the Comptroller's Findings set forth in Article II of this Order in future enforcement actions against the Bank or its institution-affiliated parties to establish a pattern or the continuation of a pattern.

(2) Nothing in this Order is a release, discharge, compromise, settlement, dismissal, or resolution of any actions, or in any way affects any actions that may be or have been brought by any other representative of the United States or an agency thereof, including, without limitation, the United States Department of Justice.

(3) This Order is:

(a) A "cease-and-desist order issued upon consent" within the meaning of 12 U.S.C. § 1818(b);

(b) A "cease-and-desist order which has become final" within the meaning of 12 U.S.C. § 1818(e);

(c) An "order issued with the consent of the depository institution" within the meaning of 12 U.S.C. § 1818(h)(2);

(d) An "effective and outstanding . . . order" within the meaning of 12 U.S.C. § 1818(i)(1); and

(e) A "final order" within the meaning of 12 U.S.C. § 1818(i)(2) and (u).

(4) This Order is effective upon its issuance by the OCC, through the Comptroller's duly authorized representative. Except as otherwise expressly provided herein, all references to "days" in this Order shall mean calendar days and the computation of any period of time imposed by this Order shall not include the date of the act or event that commences the period of time. The provisions of this Order shall remain effective except to the extent that, and until such time as, such provisions are amended, suspended, waived, or terminated in writing by the OCC, through the Comptroller's duly authorized representative. If the Bank seeks an extension, amendment, suspension, waiver, or termination of any provision of this Order, or within any plan or program submitted pursuant to this Order, the Board or a Board-designee shall submit a written request to the Deputy Comptroller asking for relief. Any request submitted pursuant to this paragraph shall include a statement setting forth in detail the special circumstances that prevent the Bank from complying with the relevant provision(s) of the Order or plan or program submitted pursuant to this Order, and shall be accompanied by relevant supporting documentation. The OCC's decision concerning a request submitted pursuant to this paragraph, which will be communicated to the Board in writing, is final and not subject to further review.

(5) The Bank will not be deemed to be in compliance with this Order until it has adopted, implemented, and adhered to all of the corrective actions set forth in each Article of this Order; the corrective actions are effective in addressing the Bank's deficiencies; and the

OCC has verified and validated the corrective actions. An assessment of the effectiveness of the corrective actions requires sufficient passage of time for the Bank to demonstrate the sustained effectiveness of the corrective actions.

(6) This Order is not a contract binding on the United States, the United States Treasury Department, the OCC, or any officer, employee, or agent of the OCC and neither the Bank nor the OCC intends this Order to be a contract.

(7) Each citation, guidance, or issuance referenced in this Order includes any subsequent citation, guidance, or issuance that replaces, supersedes, amends, or revises the referenced cited citation, guidance, or issuance.

(8) This Order applies to the Bank and all its subsidiaries.

(9) No separate promise or inducement of any kind has been made by the OCC, or by its officers, employees, or agents, to cause or induce the Bank to consent to the issuance of this Order.

(10) All reports, plans, or programs submitted to the OCC pursuant to this Order shall be forwarded, by overnight mail or via email, to the following:

Robert Barnes
Examiner-in-Charge
OCC National Bank Examiners
1600 Capital One Drive
19050-0304
Mclean, VA 22102

(11) The terms of this Order, including this paragraph, are not subject to amendment or modification by any extraneous expression, prior agreements, or prior arrangements between the parties, whether oral or written.

IN TESTIMONY WHEREOF, the undersigned, authorized by the Comptroller as his duly authorized representative, has hereunto set her signature on behalf of the Comptroller.

//s// Digitally Signed, Date: 2020.08.05

Bethany A. Dugan
Deputy Comptroller for Large Banks
Large Bank Supervision

IN TESTIMONY WHEREOF, the undersigned, as the duly elected and acting Board of Directors of Capital One, N.A. have hereunto set their signatures on behalf of Capital One, N.A.

/s/	August 01, 2020
Richard D. Fairbank	Date
/s/	July 30, 2020
R. Scott Blackley	Date
/s/	July 30, 2020
Ann Fritz Hackett	Date
/s/	July 31, 2020
Peter Thomas Killalea	Date
/s/	July 30, 2020
Francois Locoh-Donou	Date
/s/	July 30, 2020
Peter E. Raskind	Date
/s/	July 30, 2020
Mayo A. Shattuck III	Date
/s/	July 31, 2020
Sanjiv Yajnik	Date

IN TESTIMONY WHEREOF, the undersigned, as the duly elected and acting Board of Directors of Capital One Bank (USA), N.A. have hereunto set their signatures on behalf of the Capital One Bank (USA), N.A.

/s/	August 01, 2020
Richard D. Fairbank	Date
/s/	July 30, 2020
R. Scott Blackley	Date
/s/	July 30, 2020
Aparna Chennapragrada	Date
/s/	July 31, 2020
Cornelis Petrus Adrianus Joseph (“Eli”) Leenaars	Date
/s/	July 30, 2020
Pierre E. Leroy	Date
/s/	July 30, 2020
Eileen Serra	Date
/s/	July 30, 2020
Bradford H. Warner	Date
/s/	July 30, 2020
Michael J. Wassmer	Date
/s/	July 30, 2020
Catherine G. West	Date