Colin F. Campbell, 004955
Geoffrey M. T. Sturr, 014063
Timothy J. Eckstein, 018321
Joseph N. Roth, 025725
Osborn Maledon, P.A.
2929 North Central Avenue, 21st Floor
Phoenix, Arizona 85012-2793
(602) 640-9000
ccampbell@omlaw.com
gsturr@omlaw.com
teckstein@omlaw.com
jroth@omlaw.com

Attorneys for Plaintiff

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN THE COUNTY OF MARICOPA

Peter S. Davis, as Receiver of DenSco Investment Corporation, an Arizona corporation, Plaintiff, v. U.S. Bank, NA, a national banking organization; Hilda H. Chavez and John Doe Chavez, a married couple; JPMorgan Chase Bank, N.A., a national banking organization; Samantha Nelson f/k/a Samantha Kumbalek and Kristofer Nelson, a married couple; and Vikram Dadlani and Jane Doe Dadlani, a married couple, Defendants	No. CV2019-011499 **PLAINTIFF'S FIFTH SUPPLEMENTAL RULE 26.1 DISCLOSURE STATEMENT RE US BANK DEFERRAL OF PROSECUTION AND CONSENT AGREEMENTS**

For its Fifth Supplemental Disclosure Statement, Plaintiff Peter S. Davis, as Receiver of DenSco Investment Corporation, sets forth the following in addition to its prior disclosure statements:

I. FACTUAL BASIS OF CLAIMS

US Bank's Violations of Federal Law Regarding Its Anti-Money Laundering Program

During the relevant time period of the Third Amended Complaint, US Bank had a willfully deficient anti-money laundering program in violation of federal law. On February 12, 2018, US Bancorp entered into a deferred prosecution agreement with the US Government. Prosecution was deferred on a two count information charging US Bancorp with crimes: willfully failing to maintain an adequate anti-money laundering program and willfully failing to file a suspicious activity report. The deferred prosecution agreement contains a detailed statement of facts regarding the deficiencies in US Bancorps' anti-money laundering program over a period of years. The deferred prosecution agreement with the agreed statement of facts is produced with this disclosure and incorporated by reference.

US Bank entered into a consent order for a civil monetary penalty on February 13, 2018. The consent order stated:

> (a) The Bank failed to adopt and implement a compliance program that adequately covered the required BSA/AML program elements due to an inadequate system of internal controls, ineffective independent testing, and inadequate training, and the Bank failed to file all necessary Suspicious Activity Reports ("SARs") related to suspicious customer activity.
>
> (b) Some of the critical deficiencies in the elements of the Bank's BSA/AML compliance program that resulted in a violation of 12 U.S.C. § 1818(s)(3)(A) and 12 C.F.R. § 21.21, included the following:
>
> • The Bank had an inadequate system of internal controls, ineffective independent testing, and inadequate training;
>
> • The Bank had systemic deficiencies in its transaction monitoring systems, which resulted in monitoring gaps. These systemic deficiencies included the capping, or limiting, of suspicious activity alerts based on staffing considerations, which resulted in a significant amount of unreported suspicious activity; and
>
> • The Bank had systemic deficiencies in its customer due diligence processes.

(c) The Bank failed to identify certain suspicious activity and file the necessary SARs concerning suspicious customer activities, in violation of 12 C.F.R. § 21.11.

(2) The Bank conducted look-backs pursuant to the 2015 Consent Order and, as a result, had to file additional SARs which constituted additional violations of 12 C.F.R. § 21.11.

(3) The Bank violated 31 U.S.C. § 5318(i) and its implementing regulation, 31 C.F.R. § 1010.610 (correspondent banking) for deficiencies in its wire transfer monitoring in its International Banking Group.

The Consent Order for a Monetary Penalty is produced with this disclosure statement and incorporated by reference.

US Bank entered into a prior Consent Order on October 23, 2015. The consent ordered stated:

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

(1) The OCC's examination findings from 2014 and 2015 establish that the Bank has deficiencies in its BSA/AML compliance program. These deficiencies have resulted in a BSA/AML compliance program violation under 12 U.S.C. § 1818(s) and its implementing regulations 12 C.F.R. § 21.21 (BSA Compliance Program). In addition, the Bank has violated 12 C.F.R. § 21.11 (Suspicious Activity Report Filings).

(2) The Bank has failed to adopt and implement a compliance program that adequately covers the required BSA/AML program elements due to an inadequate system of internal controls, ineffective independent testing, and inadequate training, and the Bank failed to file all necessary Suspicious Activity Reports ("SARs") related to suspicious customer activity.

(3) Some of the critical deficiencies in the elements of the Bank's BSA/AML compliance program, resulting in a violation of 12 U.S.C. § 1818(s)(3)(A) and 12 C.F.R. § 21.21, include the following:

(a) The Bank has an inadequate system of internal controls, ineffective independent testing, and inadequate training.

(b) The Bank has systemic deficiencies in its transaction monitoring systems, which resulted in monitoring gaps.

(c) The Bank has systemic deficiencies in its customer due diligence processes.

(4) The Bank failed to identify certain suspicious activity and file the required SARs concerning suspicious customer activities, in violation of 12 C.F.R. § 21.11.

A copy of the Consent Order is produced with this disclosure statement and incorporated by reference.

US Bank has not produced any discovery in this case as to these matters. It did not disclose these matters in its original Rule 26.1 disclosure.

II. LEGAL BASIS OF CLAIMS

During the period of time relevant to the Third Amended Complaint, US Bank maintained a wholly inadequate anti-money laundering program. It resulted in US Bank facing a two count criminal information for violation of federal law, and the entry into a deferred prosecution agreement and consent orders as set out above.

IV. PERSONS WITH RELEVANT KNOWLEDGE

The pattern of activity for US Bank leading up to its deferred prosecution agreement includes multiple corporate officers of US Bank at the highest level of the bank. The corporate officers and other employees involved in this misconduct are material witnesses in this case. US Bank has not disclosed the names and addresses of these relevant witnesses.

VIII. EXHIBITS

The 2015 Consent Order, **R-003554-003582**.

The 2018 Consent Order, **R-003583-003597**.

The deferred prosecution agreement, **R-003598-003641**.

Assessment of Civil Money Penalty, **R-003642-003661**.

FinCEN Penalizes Compliance Officer for Anti-Money Laundering Failures article, **R-003662-003664**.

IX. RELEVANT DOCUMENTS

The 2015 Consent Order, **R-003554-003582**.

The 2018 Consent Order, **R-003583-003597**.

The deferred prosecution agreement, **R-003598-003641**.

Assessment of Civil Money Penalty, **R-003642-003661**.

FinCEN Penalizes Compliance Officer for Anti-Money Laundering Failures article, **R-003662-003664**.

DATED this 24th day of May, 2021.

OSBORN MALEDON, P.A.

By _____

Colin F. Campbell
Geoffrey M. T. Sturr
Timothy J. Eckstein
Joseph N. Roth
2929 North Central Avenue, 21st Floor
Phoenix, Arizona 85012-2793

Attorneys for Plaintiff

COPY of the foregoing served via email
this 24th day of May, 2021, on:

Greg Marshall
Amanda Z. Weaver
Bradley R. Pollock
SNELL & WILMER, L.L.P.
400 East Van Buren Street, Suite 1900
Phoenix, Arizona 85004-2202
gmarshall@swlaw.com
aweaver@swlaw.com
bpollock@swlaw.com
Attorneys for U.S. Bank National Association and Hilda Chavez

Nicole M. Goodwin
GREENBURG TRAURIG, LLP
2375 East Camelback Road, Suite 700
Phoenix, Arizona 85016
goodwinn@gtlaw.com

Paul J. Ferak
Jonathan H. Claydon
GREENBERG TRAURIG, LLP
77 West Wacker Drive, Suite 3100
Chicago, Illinois 60601
ferakp@gtlaw.com
claydonj@gtlaw.com

Attorneys for Defendant JP Morgan Chase Bank, N.A., Samantha Nelson, Kristofer Nelson, Vikram Dadlani, and Jane Doe Dadlani

8996229

VERIFICATION

Pursuant to Rule 8(h), Ariz.R.Civ.P., I, Peter S. Davis, as receiver for Plaintiff, DenSco Investment Corporation, an Arizona corporation, verify under penalty of perjury the foregoing is true and correct:

1. DenSco Investment Corporation is the Plaintiff for the above entitled action.

2. I have read the foregoing Plaintiff's Supplemental Rule 26.1 Disclosure Statement and know the contents thereof.

3. The statements and matters alleged are true of my own personal knowledge as the receiver for DenSco Investment Corporation, except as to those matters stated upon information and belief, and as to such matters, I reasonably believe them to be true.

DATED this 24th day of May, 2021.

DENSCO INVESTMENT CORPORATION, an Arizona corporation

By: Peter S. Davis
Its: Receiver

#2015-113

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

In the Matter of:	)	
U.S. Bank National Association Cincinnati, OH	)	AA-EC-2015-77

CONSENT ORDER

The Comptroller of the Currency of the United States of America ("Comptroller"), through his national bank examiners and other staff of the Office of the Comptroller of the Currency ("OCC"), has conducted examinations of U.S. Bank National Association, Cincinnati, OH ("Bank"). The OCC has identified deficiencies in the Bank's overall program for Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") compliance and has informed the Bank of the findings resulting from the examinations.

The Bank, by and through its duly elected and acting Board of Directors ("Board"), has executed a Stipulation and Consent to the Issuance of a Consent Order, dated October 23, 2015, that is accepted by the Comptroller ("Stipulation"). By this Stipulation, which is incorporated herein by reference, the Bank has consented to the issuance of this Consent Cease and Desist Order ("Order") by the Comptroller. The Bank has begun corrective action, and has committed to taking all necessary and appropriate steps to remedy the deficiencies identified by the OCC, and to enhance the Bank's BSA/AML compliance program.

ARTICLE I

COMPTROLLER'S FINDINGS

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

(1) The OCC's examination findings from 2014 and 2015 establish that the Bank has deficiencies in its BSA/AML compliance program. These deficiencies have resulted in a BSA/AML compliance program violation under 12 U.S.C. § 1818(s) and its implementing regulations 12 C.F.R. § 21.21 (BSA Compliance Program). In addition, the Bank has violated 12 C.F.R. § 21.11 (Suspicious Activity Report Filings).

(2) The Bank has failed to adopt and implement a compliance program that adequately covers the required BSA/AML program elements due to an inadequate system of internal controls, ineffective independent testing, and inadequate training, and the Bank failed to file all necessary Suspicious Activity Reports ("SARs") related to suspicious customer activity.

(3) Some of the critical deficiencies in the elements of the Bank's BSA/AML compliance program, resulting in a violation of 12 U.S.C. § 1818(s)(3)(A) and 12 C.F.R. § 21.21, include the following:

(a) The Bank has an inadequate system of internal controls, ineffective independent testing, and inadequate training.

(b) The Bank has systemic deficiencies in its transaction monitoring systems, which resulted in monitoring gaps.

(c) The Bank has systemic deficiencies in its customer due diligence processes.

(4) The Bank failed to identify certain suspicious activity and file the required SARs concerning suspicious customer activities, in violation of 12 C.F.R. § 21.11.

(5) Pursuant to the authority vested in him by the Federal Deposit Insurance Act, as amended, 12 U.S.C. § 1818(b), the Comptroller hereby ORDERS that:

ARTICLE II

COMPLIANCE COMMITTEE

(1) The Board shall appoint and maintain a Compliance Committee of at least three (3) directors of the Bank or U.S. Bancorp, of which a majority may not be employees or officers of the Bank or any of its subsidiaries or affiliates. The Compliance Committee shall be responsible for coordinating and monitoring the Bank's adherence to the provisions of this Order. The Compliance Committee shall meet at least monthly and maintain minutes of its meetings.

(2) Within one hundred twenty (120) days of the effective date of this Order, and thereafter within thirty (30) days after the end of each calendar quarter, the Compliance Committee shall submit a written progress report to the Board setting forth in detail the actions taken to comply with each Article of this Order, and the results and status of those actions, including improvements to the BSA/AML Program.

(3) The Board shall forward a copy of the Compliance Committee's report, with any additional comments by the Board, to the Examiner-in-Charge at the Bank ("Examiner-in-Charge") within ten (10) days of receiving such report.

ARTICLE III

COMPREHENSIVE BSA/AML ACTION PLAN

(1) Within ninety (90) days of the effective date of this Order, the Bank shall submit to the Examiner-in-Charge for review and determination of no supervisory objection by the Deputy Comptroller for Large Bank Supervision ("Deputy Comptroller") a plan containing a complete description of the actions that are necessary and appropriate to achieve full compliance with Articles IV through VIII of this Order ("BSA/AML Action Plan"). The Bank shall implement the BSA/AML Action Plan upon the Deputy Comptroller's issuance of a written determination of no supervisory objection. In the event the Deputy Comptroller requires the Bank to revise the plan, the Bank shall promptly make and the Board shall approve necessary and appropriate revisions and resubmit the BSA/AML Action Plan to the Examiner-in-Charge for review and determination of no supervisory objection by the Deputy Comptroller. Following implementation, the Bank shall not take any action that will cause a significant deviation from, or material change to, the BSA/AML Action Plan unless and until the Bank has received a prior written determination of no supervisory objection from the Deputy Comptroller. The Board shall ensure that the Bank achieves and thereafter maintains compliance with this Order, including, without limitation, successful implementation of the BSA/AML Action Plan. The Board shall further ensure that, upon implementation of the BSA/AML Action Plan, the Bank achieves and maintains an effective BSA/AML compliance program, in accordance with the BSA and its implementing regulations. In each instance in this Order in which the Board is required to ensure adherence to or undertake to perform certain obligations of the Bank, it is intended to mean that the Board shall:

(a) Authorize and adopt such actions on behalf of the Bank as may be necessary for the Bank to perform its obligations and undertakings;

(b) Require the timely reporting by Bank management of such actions directed by the Board to be taken under this Order;

(c) Require corrective action be taken in a timely manner for any non-compliance with such actions; and

(d) Follow-up on any non-compliance with such actions in a timely and appropriate manner.

(2) The BSA/AML Action Plan must specify timelines for completion of each of the requirements of Articles IV through VIII of this Order. The timelines in the BSA/AML Action Plan shall be consistent with any deadlines set forth in these Articles, unless modified by written agreement with the Deputy Comptroller.

(3) Upon request by the Deputy Comptroller or the Examiner-in-Charge, the Bank shall modify the BSA/AML Action Plan to address any Matters Requiring Attention concerning BSA/AML matters, or citations of violations of law concerning BSA/AML matters, which the OCC may issue to the Bank following the effective date of this Order.

(4) The Bank shall ensure that it has sufficient processes, personnel, and control systems to implement and adhere to this Order. The BSA/AML Action Plan must specify in detail staffing plans that are necessary to achieve and maintain full compliance with Articles IV through VIII of this Order.

(5) Within ten (10) days of this Order, the Bank shall designate an officer to be responsible for coordinating and submitting to the OCC the written plans, reports, and other documents required to be submitted under the terms and conditions of this Order.

ARTICLE IV

BSA/AML/OFAC COMPLIANCE PROGRAM EVALUATION

AND RISK ASSESSMENT AND COMPLIANCE PLAN

(1) Within sixty (60) days of the effective date of this Order, the Bank shall provide an action plan for the completion of an evaluation of the Bank's BSA/AML and Office of Foreign Asset Control ("OFAC") compliance programs to the Examiner-in-Charge for a written determination of no supervisory objection. If the Examiner-in-Charge recommends changes to the evaluation, the Bank shall incorporate those changes or suggest alternatives that are acceptable to the Examiner-in-Charge.

(2) The evaluation required pursuant to Paragraph (1) of this Article shall be completed and submitted to the Examiner-in-Charge within ninety (90) days following the non-objection of the Examiner-in-Charge to the action plan referred to in Paragraph (1) of this Article. This evaluation shall include assessments of the BSA/AML and OFAC compliance programs' organizational structure, enterprise-wide effectiveness, competency of management, accountability, staffing requirements, internal controls, customer due diligence processes, risk assessment processes, suspicious activity monitoring systems, sanctions screening systems, audit/independent testing, and training. The evaluation shall include recommendations for enhancements needed to achieve remediation of any deficiencies identified in the evaluation.

(3) This evaluation shall also include a comprehensive assessment of the Bank's BSA/AML risk, including detailed quantification of risk to accurately assess the level of risk and the adequacy of controls. The comprehensive assessment shall include:

(a) An assessment of the AML risk associated with each line of business, and an enterprise-wide assessment of AML risk. This evaluation shall include, but not be limited to, an assessment of the risk associated with products such as correspondent banking, pre-paid cards and mobile banking, cash vault services, and remote deposit capture, and customer types such as non-bank financial institutions, cash-intensive businesses, business, commercial, and private banking, and other higher risk products, services, customers, or geographies. The purpose of the enterprise-wide assessment is to identify systemic AML risk that may not be apparent in a risk assessment focused on line of business or assessment units;

(b) Evaluation of the Bank's current methodology for identifying and quantifying the level of BSA/AML risk associated with categories of customers and for specific customers. The methodology should ensure that the relationships are reviewed holistically, across lines of business, taking into consideration the risk within the Bank. This evaluation shall result in the development of a comprehensive, risk-based approach to quantifying BSA/AML risk for new and existing customers. The quantification of risk shall encompass a customer's entire relationship with the Bank, include the purpose of the account, actual or anticipated activity in the account (e.g., type, volume, and value (number and dollar)

of transaction activity engaged in), nature of the customer's business or occupation, customer location (e.g., customers' geographic location, where they transact business, and have significant operations), types of products and services used by the customer, material changes in the customer's relationship with the Bank, as well as other factors discussed within the FFIEC BSA/AML Examination Manual;

(c) The identification of specific lines of business, geographies, products or processes where controls are not commensurate with the level of AML risk exposure;

(d) The risk assessment shall be refreshed periodically, the timeframe for which shall not exceed twelve months, or whenever there is a significant change in AML risk within the Bank or line of business. The AML risk assessments shall also be reviewed by internal audit for the adequacy of identification of risk; control plan to manage identified risks; gap analyses where controls are not sufficient; and action plans to address gaps; and

(e) The aggregation of the Bank's enterprise-wide AML risk shall be logical and clearly supported in the work papers. The work papers and supporting documentation shall be readily accessible for OCC review.

(4) An OFAC risk assessment shall be performed annually and include the same criteria.

(5) Within ninety (90) days of completing the evaluation required pursuant to paragraph (1) of this Article, the Bank shall prepare a comprehensive BSA/AML/OFAC compliance plan that addresses all identified deficiencies and weaknesses in the Bank's

BSA/AML and OFAC compliance programs and shall submit such plan to the Examiner-in-Charge. If the Examiner-in-Charge recommends changes to such plan, the Bank shall incorporate those changes or suggest alternatives that are acceptable to the Examiner-in-Charge. The plan required by this paragraph shall then become part of the BSA/AML Action Plan required by Article III.

ARTICLE V

CUSTOMER DUE DILIGENCE

(1) Within ninety (90) days of the effective date of this Order, the Bank shall ensure that appropriate customer due diligence policies, procedures, processes, and training are developed, all in accordance with the FFIEC BSA/AML Examination Manual and other applicable regulatory guidance. These controls shall be implemented and applied on a Bank-wide basis. Minimum corporate standards shall provide enterprise-wide requirements, and individual lines of business and AML compliance management shall develop standards based on their client base, products, services, geographic risk, and other AML risk factors. Customer due diligence shall be commensurate with the customer's risk profile, and sufficient for the Bank to develop an understanding of normal and expected activity for the customer's occupation or business operations. The customer due diligence process shall include the following items:

(a) Information regarding the client's/customer's relationships with the Bank, all lines of business within the Bank, and all Bank subsidiaries or affiliates (that are subject to management control by the Banks' holding company). This includes accounts within other lines of business, regions, and countries (as permitted by jurisdiction). The relationship includes its

owners, principals, signers, subsidiaries, affiliates, and parties with the ability to manage or control the account or client (all in accordance with the FFIEC BSA/AML Examination Manual the Interagency Guidance on Beneficial Ownership Information (OCC 2010-11) and other applicable regulatory guidance);

(b) An electronic due diligence database, which includes information specified in subparagraph (a) above, that is readily accessible to the relationship manager or other parties responsible for the customer relationship, AML compliance personnel, suspicious activity monitoring alert analysts and investigators, and quality control and assurance personnel;

(c) Customer due diligence shall be periodically updated to reflect changes in the customer's behavior, activity profile, derogatory information, periodic reviews of the customer relationship, or other factors that impact the AML risk for the client and shall include any remediation required by the standards required by the Article. The periodic updates shall be documented, and subject to quality assurance processes;

(d) The client relationship AML risk shall be detailed in the customer due diligence record, along with the supporting factors, including transaction activity, geographies involved, and suspicious activity monitoring alert and filing history, among others;

(e) Specialized or enhanced due diligence for higher risk clients and/or products and services shall be implemented enterprise-wide. These due

diligence standards shall comply with the FFIEC BSA/AML Examination Manual, the Interagency Guidance on Beneficial Ownership Information (OCC 2010-11), as well as industry standards; and

(f) Management processes to periodically review, based on the relationship risk, the type, volume, and value of customer activities in relation to normal and expected levels. The purpose of these reviews shall be to determine if the customer's activity is reasonable, that customer due diligence is current and complete, and the customer risk rating is accurate. These reviews shall be documented and quality assurance processes must ensure the reviews are comprehensive and accurate. Standards and processes shall be established for elevating reviews for additional management consideration regarding increased monitoring, additional due diligence, or account closure.

(2) The Bank shall submit its policies and procedures for customer due diligence to the Examiner-in-Charge. If the Examiner-in-Charge recommends changes to the policies or procedures, the Bank shall incorporate those changes or suggest alternatives that are acceptable to the Examiner-in-Charge.

ARTICLE VI

SUSPICIOUS ACTIVITY IDENTIFICATION AND REPORTING

(1) Within ninety (90) days of this Order, the Bank shall develop and thereafter shall maintain a written program of policies and procedures to ensure, pursuant to 12 C.F.R. § 21.11,

the timely and appropriate review and disposition of BSA/AML suspicious activity alerts, and the timely filing of Suspicious Activity Reports ("SARs").

(2) Within sixty (60) days of this Order, the Bank shall evaluate its suspicious activity identification processes to ensure they are effective and provide comprehensive coverage to the Bank. This evaluation shall include an assessment of the capabilities of any surveillance and transaction monitoring systems used; the scope of coverage provided by the systems; and the management of those systems. Upon completion, the Bank shall submit this evaluation to the Examiner-in-Charge for a written determination of no supervisory objection. The evaluation shall address, but not be limited to, the following issue:

(a) An assessment of the functionality of automated transaction monitoring systems used to determine if the systems are sufficiently robust to provide for the timely identification of potentially suspicious activity. A comprehensive listing of weaknesses or deficiencies in the system, the risks presented by these deficiencies, and proposed corrective actions.

(3) Management's implementation of each surveillance and transaction monitoring system shall ensure the following:

(a) The integrity of data feeding the transaction monitoring systems;

(b) The system has been sufficiently tailored to the Bank's risk profile and operations;

(c) The system's functionality is being utilized to appropriately address risk, including the ability to aggregate data across platforms, lines of business, and relationships; and

(d) The business logic units, parameters, rules, or other factors selected for automated monitoring are appropriate and effective in identifying client activity that is unreasonable or abnormal given the nature of the client's occupation or business and expected activity. In addition, there shall be:

(i) Sufficient management information and metrics to manage and adjust the system, as necessary; and

(ii) Statistically valid processes to validate and optimize monitoring system settings and thresholds, and to measure the effectiveness of the automated system and individual scenarios, where appropriate.

(4) Management implementation of the alert investigation processes shall ensure the following:

(a) The adequacy of staffing to investigate and clear alerts;

(b) The quality and completeness of information available to analysts working transaction monitoring alerts and conducting investigations;

(c) The standards for dispositioning different types of alerts are reasonable, communicated in writing to relevant staff, and are adhered to by the alert investigators;

(d) Adequate documentation is maintained to support the disposition of alerts;

(e) The availability and adequacy of information to investigate potentially suspicious activity, including, if applicable, information from multiple lines of business a customer transacts with or information from bank subsidiaries or affiliates (that are subject to management control by the Banks' holding company);

(f) Standards that ensure accounts with high volumes of alerts are identified, elevated, and properly categorized as high risk, and subject to enhanced due diligence and monitoring;

(g) Sufficient quality control processes to ensure the surveillance and transaction monitoring system, alert management process, and SAR decisioning and filing are working effectively and according to internal standards; and

(h) The adequacy of training for staff involved in the investigation and clearing of alerts, filing of SARs, quality control and assurance processes, and management of the surveillance and transaction monitoring system.

ARTICLE VII

ACCOUNT/TRANSACTION ACTIVITY AND SUSPICIOUS ACTIVITY REPORT REVIEW ("LOOK-BACKS")

(1) Within thirty (30) days of the effective date of this Order, the Bank shall submit an acceptable action plan to the Examiner-in Charge for a written determination of no supervisory objection for conducting a review of account and transaction activity (collectively, the "Look-backs") covering areas to be specified in writing by the Examiner-in Charge.

(2) The purpose of the Look-backs is to determine whether suspicious activity was timely identified by the Bank, and, if appropriate to do so, was then timely reported by the Bank in accordance with 12 C.F.R. § 21.11.

(3) Upon completion of the Look-backs: (i) the Bank shall ensure that SARs have been filed, in accordance with 12 C.F.R. § 21.11, for any previously unreported suspicious

activity identified during this review; (ii) the written findings shall be reported to the Board; and (iii) the Bank will provide periodic and final reports to the Examiner-in-Charge, containing relevant information, identifying any SARs filed as a result of previously unreported suspicious activity.

(4) The OCC may expand the scope of the account and transaction review or require a longer account and transaction look-back period. If an additional account and transaction look-back is deemed appropriate by the OCC, the Bank shall complete the account and transaction look-back in accordance with this Article.

ARTICLE VIII

INDEPENDENT TESTING AND AUDIT

(1) Within ninety (90) days of the effective date of this Order, the Bank shall revise, implement, and maintain an effective program to audit the Bank's BSA/AML Compliance Program ("Audit Program"). The Audit Program shall include, at a minimum:

(a) A formal process to track and report upon Bank management's remediation efforts to strengthen the Bank's BSA/AML compliance program;

(b) Testing of the adequacy of internal controls designed to ensure compliance with BSA and its implementing regulations;

(c) A risk-based approach that focuses transactional testing on higher-risk clients, products, geographies, and significant relationships; and

(d) A requirement for prompt management response and follow-up to audit exceptions or other recommendations of the Bank's auditor.

(2) The Audit Program shall evaluate internal controls and effectively and timely identify non-compliance with policy, laws, rules, and regulations across lines of business and within lines of business. At least annually, the Audit Program shall evaluate the adequacy of the Bank's BSA Program based on the results of the independent testing, and considering changes in the quantity of AML risk or AML risk management.

(3) Within sixty (60) days of the effective date of this Order, the Bank shall conduct an evaluation of the adequacy of staffing of the Audit Program with respect to experience level, specialty expertise regarding BSA/AML and OFAC, and the number of the individuals employed. In addition, the Bank shall conduct an evaluation of the sufficiency of training of Audit Program staff.

(4) The Bank's Audit Program shall report all internal audit identified deficiencies to the Compliance Committee, the Bank's Audit Committee, and to senior compliance management. The reports shall indicate the severity of the deficiencies, the risks, the corrective actions, and timeframes. Corrective actions must be followed-up by internal audit within a reasonable period of time until closed. Monthly status reports on corrective action status shall be provided to the Compliance Committee and the Bank's Audit Committee.

(5) Within ninety (90) days of the effective date of this Order, the Bank shall submit the Audit Program to the Examiner-in-Charge for a prior written determination of no supervisory objection. If the Examiner-in-Charge recommends changes to the Audit Program, the Bank shall incorporate those changes or suggest alternatives that are acceptable to the Examiner-in-Charge.

ARTICLE IX

APPROVAL, IMPLEMENTATION, AND REPORTS

(1) The Bank shall submit the written plans, programs, policies, and procedures required by this Order for review and determination of no supervisory objection to the Examiner-in-Charge within the applicable time periods set forth in Articles III through VIII. The Board shall ensure that the Bank submits the plans, programs, policies, and procedures to the Examiner-in-Charge for prior written determination of no supervisory objection. In the event the Deputy Comptroller or Examiner-in-Charge asks the Bank to revise the plans, programs, policies, or procedures, the Bank shall promptly make necessary and appropriate revisions and resubmit the materials to the Examiner-in-Charge for review and determination of no supervisory objection. Upon receiving written notice of no supervisory objection from the Deputy Comptroller or Examiner-in-Charge, the Board shall ensure that the Bank implements and thereafter adheres to the plans, programs, policies, and procedures.

(2) During the term of this Order, the required plans, programs, policies, and procedures shall not be amended or rescinded in any material respect without a prior written determination of no supervisory objection from the Deputy Comptroller or Examiner-in-Charge.

(3) During the term of this Order, the Bank shall revise the required plans, programs, policies, and procedures as necessary to incorporate new, or changes to, applicable legal requirements and supervisory guidelines.

(4) The Board shall ensure that the Bank has processes, personnel, and control systems to ensure implementation of and adherence to the plans, programs, policies, and procedures required by this Order.

(5) All communication regarding this Order shall be sent to:

Grace E. Dailey
Examiner-in-Charge
National Bank Examiners
800 Nicollet Mall
Minneapolis, MN 55402-4302

or such other individuals or addresses as directed by the OCC.

ARTICLE X

OTHER PROVISIONS

(1) Although this Order requires the Bank to submit certain actions, plans, programs, and policies for the review or prior written determination of no supervisory objection by the Deputy Comptroller or the Examiner-in-Charge, the Board has the ultimate responsibility for proper and sound management of the Bank.

(2) If, at any time, the Comptroller deems it appropriate in fulfilling the responsibilities placed upon him by the several laws of the United States to undertake any action affecting the Bank, nothing in this Order shall in any way inhibit, estop, bar, or otherwise prevent the Comptroller from so doing.

(3) This Order constitutes a settlement of the cease and desist proceeding against the Bank contemplated by the Comptroller, based on the practices and violations of law or regulation described in the Comptroller's Findings set forth in Article I of this Order. The Comptroller 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 Comptroller based on the practices and violations described in Article I of the Order, to the extent known to the Comptroller as of the effective date

of the Order. Nothing in the Stipulation or this Order, however, shall prevent the Comptroller from:

(a) instituting enforcement actions, other than a cease and desist order, against the Bank based on the findings set forth in Article I of this Order;

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

(c) instituting enforcement actions against the Bank's institution-affiliated parties based on the findings set forth in Article I of this Order, or any other findings; or

(d) utilizing the findings set forth in Article I 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.

Further, nothing in the Stipulation or this Order shall affect any right of the Comptroller to determine and ensure compliance with the terms and provisions of the Stipulation and this Order.

(4) This Order is and shall become effective upon its execution by the Comptroller, through his authorized representative whose hand appears below. The Order shall remain effective and enforceable, except to the extent that, and until such time as, any provision of this Order shall be amended, suspended, waived, or terminated in writing by the Comptroller or his authorized representative.

(5) Any time limitations imposed by this Order shall begin to run from the effective date of this Order, as shown below, unless the Order specifies otherwise. The time limitations may be extended in writing by the Deputy Comptroller for good cause upon written application by the Board. Any request to extend any time limitation shall include a statement setting forth in

detail the special circumstances that prevent the Bank from complying with the time limitation, and shall be accompanied by relevant supporting documentation. The Deputy Comptroller's decision regarding the request is final and not subject to further review.

(6) The terms and provisions of this Order apply to U.S. Bank National Association and all its subsidiaries, even though those subsidiaries are not named as parties to this Order. The Bank shall integrate any activities done by a subsidiary into its plans, policies, programs, and processes required by this Order. The Bank shall ensure that its subsidiaries comply with all terms and provisions of this Order.

(7) This Order is intended to be, and shall be construed to be, a final order issued pursuant to 12 U.S.C. § 1818(b), and expressly does not form, and may not be construed to form, a contract binding the Comptroller or the United States. Without limiting the foregoing, nothing in this Order shall affect any action against the Bank or its institution-affiliated parties by a bank regulatory agency, the United States Department of Justice, or any other law enforcement agency.

(8) 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.

IT IS SO ORDERED, this _23_ day of October, 2015

S/Maryann H. Kennedy

Maryann H. Kennedy
Deputy Comptroller
Large Bank Supervision

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

In the Matter of:	)	
U.S. Bank National Association Cincinnati, OH	)	AA-EC-2015-77

STIPULATION AND CONSENT TO THE ISSUANCE OF A CONSENT ORDER

WHEREAS, the Comptroller of the Currency of the United States of America ("Comptroller"), based upon information derived from the exercise of his regulatory and supervisory responsibilities, intends to issue a cease and desist order to U.S Bank National Association, Cincinnati, OH ("Bank"), pursuant to 12 U.S.C. § 1818(b), for violations of 12 U.S.C. § 1818(s), and Bank Secrecy Act regulations, 12 C.F.R. §§ 21.11 and 21.21;

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, through its duly elected and acting Board of Directors (the "Board"), has agreed to execute this Stipulation and Consent to the Issuance of a Consent Order ("Stipulation"), that is accepted by the Comptroller, through his duly authorized representative;

NOW, THEREFORE, in consideration of the above premises, it is stipulated by the Bank that:

ARTICLE I

JURISDICTION

(1) The Bank is a national banking association chartered and examined by the Comptroller pursuant to the National Bank Act of 1864, as amended, 12 U.S.C. § 1 *et seq*.

(2) The Comptroller is "the appropriate Federal banking agency" regarding the Bank pursuant to 12 U.S.C. §§ 1813(q) and 1818(b).

(3) The Bank is an "insured depository institution" within the meaning of 12 U.S.C. § 1818(b)(1).

ARTICLE II

CONSENT

(1) The Bank, without admitting or denying any wrongdoing, consents and agrees to issuance of the accompanying Consent Order by the Comptroller.

(2) The terms and provisions of the Consent Order apply to the Bank and all of its subsidiaries, even though those subsidiaries are not named as parties to the Consent Order.

(3) The Bank consents and agrees that the Consent Order shall be deemed an "order issued with the consent of the depository institution" pursuant to 12 U.S.C. § 1818(h)(2), and consents and agrees that the Consent Order shall become effective upon its execution by the Comptroller through his authorized representative, and shall be fully enforceable by the Comptroller pursuant to 12 U.S.C. § 1818(i).

(4) Notwithstanding the absence of mutuality of obligation, or of consideration, or of a contract, the Comptroller may enforce any of the commitments or obligations herein undertaken by the Bank under his supervisory powers, including 12 U.S.C. § 1818(b), and not as

a matter of contract law. The Bank expressly acknowledges that neither the Bank nor the Comptroller has any intention to enter into a contract.

(5) The Bank declares that no separate promise or inducement of any kind has been made by the Comptroller, or by his agents or employees, to cause or induce the Bank to consent to the issuance of the Consent Order and/or execute this Stipulation.

(6) The Bank expressly acknowledges that no officer or employee of the Comptroller has statutory or other authority to bind the United States, the United States Treasury Department, the Comptroller, or any other federal bank regulatory agency or entity, or any officer or employee of any of those entities to a contract affecting the Comptroller's exercise of his supervisory responsibilities.

(7) The Consent Order constitutes a settlement of the cease and desist proceeding against the Bank contemplated by the Comptroller, based on the practices and violations of law described in the Comptroller's Findings set forth in Article I of the Consent Order. The Comptroller 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 Comptroller based on the practices and violations described in Article I of the Consent Order, to the extent known to the Comptroller as of the effective date of the Consent Order. Nothing in this Stipulation or the Consent Order, however, shall prevent the Comptroller from:

(a) instituting enforcement actions other than a cease and desist order against the Bank based on the findings set forth in Article I of the Consent Order;

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

(c) instituting enforcement actions against the Bank's institution-affiliated parties based on the findings set forth in Article I of the Consent Order, or any other findings; or

(d) utilizing the findings set forth in Article I of the Consent Order in future enforcement actions against the Bank or its institution-affiliated parties to establish a pattern or the continuation of a pattern.

Further, nothing in this Stipulation or the Consent Order shall affect any right of the Comptroller to determine and ensure compliance with the terms and provisions of this Stipulation or the Consent Order.

ARTICLE III

WAIVERS

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

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

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

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

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

(e) Any and all claims for fees, costs, or expenses against the Comptroller, or any of his agents or employees, related in any way to this enforcement

matter or the Consent 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, this Stipulation, consent to the issuance of the Consent Order, and/or the issuance of the Consent 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 the Consent Order.

ARTICLE IV

ELIGIBLE BANK – OTHER PROVISIONS

(1) As a result of the Consent Order:

(a) The Bank is an "eligible bank" pursuant to 12 C.F.R. § 5.3(g)(4) for the purposes of 12 C.F.R. Part 5 regarding rules, policies and procedures for corporate activities, unless otherwise informed in writing by the Office of the Comptroller of the Currency ("OCC");

(b) The Bank is not subject to the limitation of 12 C.F.R. § 5.51(c)(6)(ii) for the purposes of 12 C.F.R. § 5.51 requiring OCC approval of a change in directors and senior executive officers, unless otherwise informed in writing by the OCC;

(c) The Bank is not subject to the limitation on golden parachute and indemnification payments provided by 12 C.F.R. § 359.1(f)(1)(ii)(C) and

12 C.F.R. § 5.51(c)(6)(ii), unless otherwise informed in writing by the OCC;

(d) The Bank's status as an "eligible bank" remains unchanged pursuant to 12 C.F.R. § 24.2(e)(4) for the purposes of 12 C.F.R. Part 24 regarding community and economic development, unless otherwise informed in writing by the OCC; and

(e) The Consent Order shall not be construed to be a "written agreement, order, or capital directive" within the meaning of 12 C.F.R. § 6.4, unless the OCC informs the Bank otherwise in writing.

ARTICLE V

CLOSING

(1) The provisions of this Stipulation and the Consent Order shall not inhibit, estop, bar, or otherwise prevent the Comptroller from taking any other action affecting the Bank if, at any time, he deems it appropriate to do so to fulfill the responsibilities placed upon him by the several laws of the United States of America.

(2) Nothing in this Stipulation or the Consent Order shall preclude any proceedings brought by the Comptroller to enforce the terms of the Consent Order, and nothing in this Stipulation or the Consent Order constitutes, nor shall the Bank contend that it constitutes, 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) The terms of this Stipulation, including this paragraph, and of the Consent Order 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 representative, has hereunto set his hand on behalf of the Comptroller.

S/Maryann H. Kennedy — 10/23/15

Maryann H. Kennedy
Deputy Comptroller
Large Bank Supervision

Date

IN TESTIMONY WHEREOF, the undersigned, as the duly elected and acting Board of Directors of U.S. Bank National Association, have hereunto set their hands on behalf of the Bank.

S/Richard K. Davis	10/13/15
Richard K. Davis	Date
S/Jennie P. Carlson	10/13/15
Jennie P. Carlson	Date
S/Andrew Cecere	10/13/15
Andrew Cecere	Date
S/James L. Chosy	10/14/15
James L. Chosy	Date
S/Terrance R. Dolan	10/14/15
Terrance R. Dolan	Date
S/John R. Elmore	10/13/15
John R. Elmore	Date
S/Roland A. Hernandez	10/14/15
Roland A. Hernandez	Date
S/Shailesh M. Kotwal	10/13/2015
Shailesh M. Kotwal	Date

S/P.W. (Bill) Parker	10/13/2015
P. W. (Bill) Parker	Date
S/Richard B. Payne, Jr.	10/13/15
Richard B. Payne, Jr.	Date
S/Katherine B. Quinn	10/13/15
Katherine B. Quinn	Date
S/Kathleen A. Rogers	10/13/15
Kathleen A. Rogers	Date
S/Mark G. Runkel	10/13/15
Mark G. Runkel	Date
S/Craig D. Schnuck	10/13/15
Craig D. Schnuck	Date
S/Kent v. Stone	10/13/15
Kent V. Stone	Date
S/Jeffry H. von Gillern	10/14/2015
Jeffry H. von Gillern	

#2018-010

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

In the Matter of:	)	
U.S. Bank National Association Cincinnati, OH	)	AA-EC-2018-84

CONSENT ORDER FOR A CIVIL MONEY PENALTY

The Comptroller of the Currency of the United States of America ("Comptroller"), through his national bank examiners and other staff of the Office of the Comptroller of the Currency ("OCC"), conducted examinations of U.S. Bank National Association, Cincinnati, OH ("Bank"). The OCC identified deficiencies in the Bank's Bank Secrecy Act/anti-money laundering ("BSA/AML") compliance program that resulted in violations of 12 U.S.C. § 1818(s) and its implementing regulation, 12 C.F.R. § 21.21, 12 C.F.R. § 21.11, and 31 U.S.C. § 5318(i) and its implementing regulation, 31 C.F.R. § 1010.610, and informed the Bank of the findings resulting from the examinations. The OCC issued a Consent Cease and Desist Order for the BSA/AML deficiencies on October 23, 2015 ("2015 Consent Order").

The Bank, by and through its duly elected and acting Board of Directors ("Board"), has executed a Stipulation and Consent to the Issuance of an Order for a Civil Money Penalty, dated February 13, 2018 that is accepted by the Comptroller ("Stipulation"). By this Stipulation, which is incorporated herein by reference, the Bank has consented to the issuance of this Consent Order for a Civil Money Penalty ("Order") by the Comptroller. The Bank has undertaken corrective action, and is committed to taking all necessary and appropriate steps to remedy the deficiencies identified by the OCC and to enhance the Bank's BSA/AML program.

ARTICLE I

COMPTROLLER'S FINDINGS

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

(1) In the 2015 Consent Order, the Comptroller found that the Bank violated 12 U.S.C. § 1818(s) and its implementing regulation, 12 C.F.R. § 21.21 (BSA/AML compliance program), and 12 C.F.R. § 21.11 (suspicious activity report filings). Specifically, the 2015 Consent Order addressed the following conduct:

(a) The Bank failed to adopt and implement a compliance program that adequately covered the required BSA/AML program elements due to an inadequate system of internal controls, ineffective independent testing, and inadequate training, and the Bank failed to file all necessary Suspicious Activity Reports ("SARs") related to suspicious customer activity.

(b) Some of the critical deficiencies in the elements of the Bank's BSA/AML compliance program that resulted in a violation of 12 U.S.C. § 1818(s)(3)(A) and 12 C.F.R. § 21.21, included the following:

- The Bank had an inadequate system of internal controls, ineffective independent testing, and inadequate training;
- The Bank had systemic deficiencies in its transaction monitoring systems, which resulted in monitoring gaps. These systemic deficiencies included the capping, or limiting, of suspicious activity alerts based on staffing considerations,

which resulted in a significant amount of unreported suspicious activity; and

- The Bank had systemic deficiencies in its customer due diligence processes.

(c) The Bank failed to identify certain suspicious activity and file the necessary SARs concerning suspicious customer activities, in violation of 12 C.F.R. § 21.11.

(2) The Bank conducted look-backs pursuant to the 2015 Consent Order and, as a result, had to file additional SARs which constituted additional violations of 12 C.F.R. § 21.11.

(3) The Bank violated 31 U.S.C. § 5318(i) and its implementing regulation, 31 C.F.R. § 1010.610 (correspondent banking) for deficiencies in its wire transfer monitoring in its International Banking Group.

(4) Pursuant to the authority vested in him by the Federal Deposit Insurance Act, as amended, 12 U.S.C. § 1818, the Comptroller hereby ORDERS that:

ARTICLE II

ORDER FOR A CIVIL MONEY PENALTY

Pursuant to the authority vested in him by the Federal Deposit Insurance Act, 12 U.S.C. § 1818(i), the Comptroller orders, and the Bank consents to the following:

(1) The Bank shall make payment of a civil money penalty in the total amount of seventy-five million dollars ($75,000,000), which shall be paid upon the execution of this Order:

(a) If a check is the selected method of payment, the check shall be made payable to the Treasurer of the United States and shall be delivered to: Comptroller of the Currency, P.O. Box 979012, St. Louis, Missouri 63197-9000.

(b) If a wire transfer is the selected method of payment, it shall be sent in accordance with instructions provided by the Comptroller.

(c) The docket number of this case (AA-EC-2018-84) shall be entered on the payment document or wire confirmation and a photocopy of the payment document or confirmation of the wire transfer shall be sent immediately, by overnight delivery, to the Director of Enforcement and Compliance, Office of the Comptroller of the Currency, 400 7th Street, S.W., Washington, D.C. 20219.

(2) This Order shall be enforceable to the same extent and in the same manner as an effective and outstanding order that has been issued and has become final pursuant to 12 U.S.C. § 1818(h) and (i).

ARTICLE III

OTHER PROVISIONS

(1) This Order is intended to be, and shall be construed to be, a final order issued pursuant to 12 U.S.C. § 1818(i)(2), and expressly does not form, and may not be construed to form, a contract binding on the Comptroller or the United States.

(2) This Order constitutes a settlement of the civil money penalty proceeding against the Bank contemplated by the Comptroller, based on the practices and violations described in the Comptroller's Findings set forth in Article I of this Order. The Comptroller releases and

discharges the Bank from all potential liability for a civil money penalty that has been or might have been asserted by the Comptroller based on the practices and violations described in Article I of this Order, to the extent known to the Comptroller as of the effective date of this Order. Nothing in the Stipulation or this Order, however, shall prevent the Comptroller from:

(a) instituting enforcement actions other than a civil money penalty against the Bank based on the findings set forth in Article I of this Order;

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

(c) instituting enforcement actions against the Bank's institution-affiliated parties based on the findings set forth in Article I of this Order, or any other findings; or

(d) utilizing the findings set forth in Article I 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.

Further, nothing in the Stipulation or this Order shall affect any right of the Comptroller to determine and ensure compliance with the terms and provisions of the Stipulation or this Order.

(3) 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.

IT IS SO ORDERED, this 13th day of February 2018.

/s/
Maryann H. Kennedy
Deputy Comptroller
Large Bank Supervision

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

In the Matter of:	)	
U.S. Bank National Association Cincinnati, OH	)	AA-EC-2018-84

STIPULATION AND CONSENT TO THE ISSUANCE OF AN ORDER FOR A CIVIL MONEY PENALTY

WHEREAS, the Comptroller of the Currency of the United States of America ("Comptroller"), based upon information derived from the exercise of his regulatory and supervisory responsibilities, intends to initiate a civil money penalty proceeding against U.S. Bank National Association, Cincinnati, OH ("Bank"), pursuant to 12 U.S.C. § 1818(i), for the Bank's violations of 12 U.S.C. § 1818(s) and its implementing regulation, 12 C.F.R. § 21.21, 12 C.F.R. § 21.11, and 31 U.S.C. § 5318(i) and its implementing regulation, 31 C.F.R. § 1010.610;

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, through its duly elected and acting Board of Directors ("Board"), has agreed to execute this Stipulation and Consent to the Issuance of a Civil Money Penalty ("Stipulation"), that is accepted by the Comptroller, through his duly authorized representative;

NOW, THEREFORE, in consideration of the above premises, it is stipulated by the Bank that:

ARTICLE I

JURISDICTION

(1) The Bank is a national banking association chartered and examined by the Comptroller pursuant to the National Bank Act of 1864, as amended, 12 U.S.C. § 1 *et seq.*

(2) The Comptroller is "the appropriate Federal banking agency" regarding the Bank pursuant to 12 U.S.C. §§ 1813(q) and 1818(i).

(3) The Bank is an "insured depository institution" within the meaning of 12 U.S.C. § 1818(i).

ARTICLE II

CONSENT

(1) The Bank, without admitting or denying any wrongdoing, consents and agrees to issuance of the accompanying Consent Order for a Civil Money Penalty ("Consent Order") by the Comptroller.

(2) The terms and provisions of the Consent Order apply to the Bank and all of its subsidiaries, even though those subsidiaries are not named as parties to the Consent Order.

(3) The Bank consents and agrees that the Consent Order shall be deemed an "order issued with the consent of the depository institution" pursuant to 12 U.S.C. § 1818(h)(2), and consents and agrees that the Consent Order shall become effective upon its execution by the Comptroller through his authorized representative, and shall be fully enforceable by the Comptroller pursuant to 12 U.S.C. § 1818(i).

(4) Notwithstanding the absence of mutuality of obligation, or of consideration, or of a contract, the Comptroller may enforce any of the commitments or obligations herein

undertaken by the Bank under his supervisory powers, including 12 U.S.C. § 1818(i), and not as a matter of contract law. The Bank expressly acknowledges that neither the Bank nor the Comptroller has any intention to enter into a contract.

(5) The Bank declares that no separate promise or inducement of any kind has been made by the Comptroller, or by his agents or employees, to cause or induce the Bank to consent to the issuance of the Consent Order and/or execute this Stipulation.

(6) The Bank expressly acknowledges that no officer or employee of the Comptroller has statutory or other authority to bind the United States, the United States Treasury Department, the Comptroller, or any other federal bank regulatory agency or entity, or any officer or employee of any of those entities to a contract affecting the Comptroller's exercise of his supervisory responsibilities.

(7) The Consent Order constitutes a settlement of the civil money penalty proceeding against the Bank contemplated by the Comptroller, based on the practices and violations described in the Comptroller's Findings set forth in Article I of the Consent Order. The Comptroller releases and discharges the Bank from all potential liability for a civil money penalty that has been or might have been asserted by the Comptroller based on the practices and violations described in Article I of the Consent Order, to the extent known to the Comptroller as of the effective date of the Consent Order. Nothing in this Stipulation or the Consent Order, however, shall prevent the Comptroller from:

(a) instituting enforcement actions other than a civil money penalty against the Bank based on the findings set forth in Article I of the Consent Order;

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

(c) instituting enforcement actions against the Bank's institution-affiliated parties based on the findings set forth in Article I of the Consent Order, or any other findings; or

(d) utilizing the findings set forth in Article I of the Consent Order in future enforcement actions against the Bank or its institution-affiliated parties to establish a pattern or the continuation of a pattern.

Further, nothing in this Stipulation or the Consent Order shall affect any right of the Comptroller to determine and ensure compliance with the terms and provisions of this Stipulation or the Consent Order.

ARTICLE III

WAIVERS

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

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

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

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

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

(e) Any and all claims for fees, costs or expenses against the Comptroller, or any of his agents or employees, related in any way to this enforcement matter or the Consent 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, this Stipulation, consent to the issuance of the Consent Order, and/or the issuance of the Consent 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 the Consent Order.

ARTICLE IV

CLOSING

(1) The provisions of this Stipulation and the Consent Order shall not inhibit, estop, bar, or otherwise prevent the Comptroller from taking any other action affecting the Bank if, at any time, he deems it appropriate to do so to fulfill the responsibilities placed upon him by the several laws of the United States of America.

(2) Nothing in this Stipulation or the Consent Order shall preclude any proceedings brought by the Comptroller to enforce the terms of the Consent Order, and nothing in this

Stipulation or the Consent Order constitutes, nor shall the Bank contend that it constitutes, 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) The terms of this Stipulation, including this paragraph, and of the Consent Order 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, as the duly elected and acting Board of Directors of U.S. Bank National Association, Cincinnati, OH, have hereunto set their hands on behalf of the Bank.

/s/	2/13/18
Jennie P. Carlson	Date
/s	2/13/18
Andrew Cecere	Date
/s/	2/13/18
James L. Chosy	Date
/s/	2/13/18
Terrance R. Dolan	Date
/s/	2/13/18
John R. Elmore	Date
/s/	2/13/18
Leslie V. Godridge	Date
/s/	2/13/18
Gunjan Kedia	Date
/s/	2/13/18
James B. Kelligrew	Date
/s/	2/13/18
Shailesh M. Kotwal	Date
/s/	2/13/18
Karen S. Lynch	Date

/s/	2/13/18
P.W. (Bill) Parker	Date
/s/	2/13/18
Katherine B. Quinn	Date
/s/	2/13/18
Mark G. Runkel	Date
/s/	2/13/18
Jeffry H. von Gillern	Date
/s/	2/13/18
Timothy A. Welsh	Date
/s/	2/13/18
Scott W. Wine	Date

Accepted by:

THE COMPTROLLER OF THE CURRENCY

/s/
Maryann H. Kennedy
Deputy Comptroller
Large Bank Supervision

2/13/18
Date

EX-10.1 2 d516835dex101.htm EX-10.1

Exhibit 10.1

U.S. Department of Justice

United States Attorney

Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York New York 10007

February 12, 2018

Boyd M. Johnson III, Esq.
Wilmer Hale LLP
7 World Trade Center
New York, NY 10007

Samuel W. Seymour, Esq.
Sullivan & Cromwell LLP
125 Broad Street
New York, NY 10004

Re: U.S. Bancorp – Deferred Prosecution Agreement

Dear Messrs. Johnson and Seymour:

Pursuant to the understandings specified below, the Office of the United States Attorney for the Southern District of New York (the "Office") and defendant U.S. Bancorp ("USB"), under authority granted by its Board of Directors in the form of a Board Resolution (a copy of which is attached hereto as Exhibit A), hereby enter into this Deferred Prosecution Agreement (the "Agreement").

The Criminal Information

1. USB consents to the filing of a two-count Information (the "Information") in the United States District Court for the Southern District of New York (the "Court"), charging USB with willfully failing to maintain an adequate anti-money laundering ("AML") program, in violation of Title 31, United States Code, Sections 5318(h) and 5322(a) and (c) and Title 31, Code of Federal Regulations, Section 1020.210, and willfully failing to file a Suspicious Activity Report, in violation of Title 31, United States Code, Sections 5318(g) and 5322(a) and (c) and Title 31, Code of Federal Regulations, Section 1020.320. A copy of the Information is attached hereto as Exhibit B. This Agreement shall take effect upon its execution by both parties.

Acceptance of Responsibility

2. USB stipulates that the facts set forth in the Statement of Facts, attached hereto as Exhibit C and incorporated herein, are true and accurate, and admits, accepts and acknowledges that it is responsible under United States law for the acts of its current and former officers and employees as set forth in the Statement of Facts. Should the Office pursue the prosecution that is deferred by this Agreement, USB stipulates to the admissibility of the Statement of Facts in any proceeding including any trial and sentencing proceeding.

Boyd M. Johnson, Esq.
Samuel W. Seymour, Esq.
February 12, 2018

Payments and Forfeiture Obligation

3. As a result of the conduct described in the Information and the Statement of Facts, USB agrees to pay $528,000,000 to the United States, less the amount of any civil money penalty paid by USB to the Office of the Comptroller of the Currency ("OCC") in connection with its concurrent settlement of the related regulatory action brought by the OCC (the "Stipulated Forfeiture Amount"), pursuant to this Agreement.

4. USB agrees that the Stipulated Forfeiture Amount represents a substitute *res* for funds received and/or transferred by Scott Tucker ("Tucker") through USB or its subsidiaries in connection with the conduct described in the Statement of Facts, and is subject to civil forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) and (a)(1)(C).

5. USB further agrees that this Agreement, the Information and the Statement of Facts may be attached and incorporated into a civil forfeiture complaint (the "Civil Forfeiture Complaint") that will be filed against the Stipulated Forfeiture Amount. By this agreement, USB expressly waives any challenge to that Civil Forfeiture Complaint and consents to the forfeiture of the Stipulated Forfeiture Amount to the United States. USB agrees that it will not file a claim with the Court or otherwise contest the civil forfeiture of the Stipulated Forfeiture Amount and will not assist a third party in asserting any claim to the Stipulated Forfeiture Amount. USB also waives all rights to service or notice of the Civil Forfeiture Complaint.

6. USB shall transfer the Stipulated Forfeiture Amount to the United States by no later than February 15, 2018 (or as otherwise directed by the Office following such date). Such payment shall be made by wire transfer to the United States Treasury, pursuant to wire instructions provided by the Office. If USB fails to timely make the payment required under this paragraph, interest (at the rate specified in Title 28, United States Code, Section 1961) shall accrue on the unpaid balance through the date of payment, unless the Office, in its sole discretion, chooses to reinstate prosecution pursuant to paragraphs 13 and 14 below. USB certifies that the funds used to pay the Stipulated Forfeiture Amount are not the subject of any lien, security agreement, or other encumbrance. Transferring encumbered funds or failing to pass clean title to these funds in any way will be considered a breach of this Agreement.

7. USB agrees that the Stipulated Forfeiture Amount shall be treated as a penalty paid to the United States government for all purposes, including all tax purposes. USB agrees that it will not claim, assert, or apply for a tax deduction or tax credit with regard to any federal, state, local, or foreign tax for any portion of the up to $528,000,000 that USB has agreed to pay to the United States pursuant to this Agreement.

Obligation to Cooperate

8. USB agrees to cooperate fully with the Office, the Internal Revenue Service ("IRS"), the OCC, the Financial Crimes Enforcement Network ("FinCEN") and any other governmental agency designated by the Office regarding any matter relating to the conduct described in the Information or Statement of Facts, or any matter relating to the payday lending scheme perpetrated by Tucker and the companies he owned and controlled.

9. It is understood that USB shall (a) truthfully and completely disclose all information with respect to the activities of USB and its officers, agents, affiliates and employees concerning all matters about which the Office inquires of it, which information can be used for any purpose; (b) cooperate fully with the Office, IRS, OCC, FinCEN and any other governmental agency designated by the Office; (c) attend all meetings at which the Office requests its presence and use its reasonable best efforts to secure the attendance and truthful statements or testimony of any past or current officers, agents, or employees of USB at any meeting or interview or before the grand jury or at trial or at any other court proceeding; (d) provide to the Office upon request any document, record, or other tangible evidence relating to matters about which the Office or any designated law enforcement agency inquires of it; (e) assemble, organize, and provide in a responsive and prompt fashion, and upon request, on an expedited schedule, all documents, records, information and other evidence in USB's possession, custody or control as may be requested by the Office, IRS, OCC, FinCEN or designated governmental agency; (f) volunteer and provide to the Office any information and documents that come to USB's attention that may be relevant to the Office's investigation of this matter or any issue related to the Statement of Facts, as designated by the Office; (g) provide testimony or information necessary to identify or establish the original location, authenticity, or other basis for admission into evidence of documents or physical evidence in any criminal or other proceeding as requested by the Office, IRS, OCC, FinCEN or designated governmental agency, including but not limited to information and testimony concerning the conduct set forth in the Information and Statement of Facts; (h) bring to the Office's attention all criminal conduct by USB or any of its agents or employees acting within the scope of their employment related to violations of the federal laws of the United States, as to which USB's Board of Directors, senior management, or United States legal and compliance personnel are aware; (i) bring to the Office's attention any administrative, regulatory, civil or criminal proceeding or investigation of USB or any agents or employees acting within the scope of their employment relating to United States sanctions or AML laws; and (j) commit no crimes whatsoever under the federal laws of the United States subsequent to the execution of this Agreement. Nothing in this Agreement shall be construed to require USB to provide information, documents, or testimony protected by the attorney-client privilege, work product doctrine, or other applicable privileges.

10. USB agrees that its obligations pursuant to this Agreement, which shall commence upon the signing of this Agreement, will continue for two years from the date of the Court's acceptance of this Agreement, unless otherwise extended pursuant to paragraph 15 below. USB's obligation to cooperate is not intended to apply in the event that a prosecution against USB by this Office is pursued and not deferred.

Deferral of Prosecution

11. In consideration of USB's entry into this Agreement and its commitment to: (a) accept and acknowledge responsibility for the conduct described in the Statement of Facts and the Information; (b) cooperate with the Office, IRS, OCC, FinCEN and any other law enforcement agency designated by this Office; (c) make the payment specified in this Agreement;

(d) comply with Federal criminal laws (as provided herein in paragraph 9); and (e) otherwise comply with all of the terms of this Agreement, the Office agrees that prosecution of USB on the Information be and hereby is deferred for two years from the date of the signing of this Agreement. USB shall expressly waive indictment and all rights to a speedy trial pursuant to the Sixth Amendment of the United States Constitution, Title 18, United States Code, Section 3161, Federal Rule of Criminal Procedure 48(b), and any applicable Local Rules of the United States District Court for the Southern District of New York for the period during which this Agreement is in effect.

12. It is understood that this Office cannot, and does not, agree not to prosecute USB for criminal tax violations. However, if USB fully complies with the terms of this Agreement, no testimony given or other information provided by USB (or any other information directly or indirectly derived therefrom) will be used against USB in any criminal tax prosecution. In addition, the Office agrees that, if USB is in compliance with all of its obligations under this Agreement, the Office will, within thirty (30) days after the expiration of the period of deferral (including any extensions thereof), seek dismissal with prejudice of the Information filed against USB pursuant to this Agreement. Except in the event of a violation by USB of any term of this Agreement or as otherwise provided in paragraph 13, the Office will bring no additional charges against USB or its subsidiaries, except for criminal tax violations, relating to conduct described in the Statement of Facts or otherwise disclosed to the Office during its investigation of this matter. This Agreement does not provide any protection against prosecution for any crimes except as set forth above and does not apply to any individual or entity other than USB and its subsidiaries. USB and the Office understand that the Agreement to defer prosecution of USB can only operate as intended if the Court grants a waiver of the Speedy Trial Act pursuant to 18 U.S.C. § 3161(h)(2). Should the Court decline to do so, both the Office and USB are released from any obligation imposed upon them by this Agreement, and this Agreement shall be null and void, except for the tolling provision set forth in paragraph 13.

13. It is further understood that should the Office in its sole discretion determine that USB has: (a) knowingly given false, incomplete or misleading information either during the term of this Agreement or in connection with the Office's investigation of the conduct described in the Information and Statement of Facts, (b) committed any crime under the federal laws of the United States subsequent to the execution of this Agreement, or (c) otherwise violated any provision of this Agreement, USB shall, in the Office's sole discretion, thereafter be subject to prosecution for any federal criminal violation, or suit for any civil cause of action, of which the Office has knowledge, including but not limited to a prosecution or civil action based on the Information, the Statement of Facts, the conduct described therein, or perjury and obstruction of justice. Any such prosecution or civil action may be premised on any information provided by or on behalf of USB to the Office, IRS, OCC or FinCEN at any time. In any such prosecution or civil action, it is understood that: (a) no charge or claim would be time-barred provided that such prosecution or civil action is brought within the applicable statute of limitations period (subject to any prior tolling agreements between the Office and USB), excluding the period from the execution of this Agreement until its termination; (b) USB agrees to toll, and exclude from any calculation of time, the running of the applicable statute of limitations for the length of this Agreement starting from the date of the execution of this Agreement and including any extension of the period of deferral of prosecution pursuant to paragraph 15 below; and (c) USB waives any objection to venue with

respect to any charges arising out of the conduct described in the Statement of Facts and consents to the filing of such charges in the Southern District of New York. By this Agreement, USB expressly intends to and hereby does waive its rights in the foregoing respects, including any right to make a claim premised on the statute of limitations, as well as any constitutional, statutory, or other claim concerning pre-indictment delay. Such waivers are knowing, voluntary, and in express reliance on the advice of USB's counsel.

14. It is further agreed that in the event that the Office, in its sole discretion, determines that USB has violated any provision of this Agreement, including by failure to meet its obligations under this Agreement: (a) USB shall not object to the admissibility of all statements made or acknowledged by or on behalf of USB to the Office, IRS, OCC, or FinCEN, including but not limited to the Statement of Facts, or any testimony given by USB or by any agent of USB before a grand jury, or elsewhere, whether before or after the date of this Agreement, or any leads from such statements or testimony, in any and all criminal proceedings hereinafter brought by the Office against USB; and (b) USB shall not assert any claim under the United States Constitution, Rule 11(f) of the Federal Rules of Criminal Procedure, Rule 410 of the Federal Rules of Evidence, or any other federal rule, that statements made or acknowledged by or on behalf of USB before or after the date of this Agreement, or any leads derived therefrom, should be suppressed or otherwise excluded from evidence. It is the intent of this Agreement to waive any and all rights in the foregoing respects.

15. USB agrees that, in the event that the Office determines during the period of deferral of prosecution described in paragraph 10 above (or any extensions thereof) that USB has violated any provision of this Agreement, an extension of the period of deferral of prosecution may be imposed in the sole discretion of the Office, up to an additional one year, but in no event shall the total term of the deferral-of-prosecution period of this Agreement exceed three (3) years. Any extension of the deferral-of-prosecution period extends all terms of this Agreement for an equivalent period.

16. USB, having truthfully admitted to the facts in the Statement of Facts, agrees that it shall not, through its attorneys, agents, or employees, make any statement, in litigation or otherwise, contradicting the Statement of Facts or its representations in this Agreement. Consistent with this provision, USB may raise defenses and/or assert affirmative claims in any proceedings brought by private and/or public parties as long as doing so does not contradict the Statement of Facts or such representations. Any such contradictory statement by USB, its present or future attorneys, agents, or employees shall constitute a violation of this Agreement and USB thereafter shall be subject to prosecution as specified in paragraphs 13 through 14, above, or the deferral-of-prosecution period shall be extended pursuant to paragraph 15, above. The decision as to whether any such contradictory statement will be imputed to USB for the purpose of determining whether USB has violated this Agreement shall be within the sole discretion of the Office. Upon the Office's notifying USB of any such contradictory statement, USB may avoid a finding of violation of this Agreement by repudiating such statement both to the recipient of such statement and to the Office within five business days after having been provided notice by the Office. USB consents to the public release by the Office, in its sole discretion, of any such repudiation. Nothing in this Agreement is meant to affect the obligation of USB or its officers, directors, agents or employees to testify truthfully in any proceeding.

17. USB agrees that it is within the Office's sole discretion to choose, in the event of a violation, the remedies contained in paragraphs 13 and 14 above, or instead to choose to extend the period of deferral of prosecution pursuant to paragraph 15, provided, however, that if USB's violation of this Agreement is limited to an untimely payment of the Stipulated Forfeiture Amount, the Office may elect instead to choose the additional financial penalties set forth in paragraph 6, above. USB understands and agrees that the exercise of the Office's discretion under this Agreement is unreviewable by any court. Should the Office determine that USB has violated this Agreement, the Office shall provide notice to USB of that determination and provide USB with an opportunity to make a presentation to the Office to demonstrate that no violation occurred, or, to the extent applicable, that the violation should not result in the exercise of any of those remedies, including because the violation has been cured by USB.

The Bank's BSA/AML Compliance Program

18. U.S. Bank National Association (the "Bank") shall continue its ongoing effort to implement and maintain an adequate Bank Secrecy Act ("BSA")/AML compliance program in accordance with the BSA, its implementing regulations, and the directives and orders of any United States regulator of the Bank, including without limitation the OCC, as set forth in the OCC's Consent Order dated October 23, 2015. The Office acknowledges that, prior to the entry of this Agreement, the Bank has implemented and is continuing to implement significant remedial changes to its BSA/AML compliance program. It is understood that a violation of the BSA or the Consent Order arising from conduct exclusively occurring prior to the date of execution of this Agreement will not constitute a breach of USB's obligations pursuant to this Agreement. However, there shall be no limitation on the ability of the Office to investigate or prosecute such violations and/or conduct in accordance with the applicable law and the other terms of this Agreement, including paragraph 12 hereof.

Review of the Bank's BSA/AML Compliance Program

19. For the duration of the Agreement, USB shall provide the Office with semi- annual reports ("Semi-Annual Reports") describing the status of the Bank's implementation of the remedial changes to its BSA/AML compliance program required by the Consent Order. The Semi- Annual Reports shall identify any violations of the BSA that have come to the attention of the Bank's legal and compliance personnel during this reporting period.

20. For the duration of this Agreement, the Office, as it deems necessary and upon request to USB, shall: (a) be provided by USB with access to any and all non-privileged books, records, accounts, correspondence, files, and any and all other documents or other electronic records, including e-mails, of USB and its representatives, agents, affiliates, and employees, relating to any matters described or identified in the Semi-Annual Reports; and (b) have the right to interview any officer, employee, agent, consultant, or representative of USB concerning any non- privileged matter described or identified in the Semi-Annual Reports.

21. It is understood that USB shall promptly notify the Office of (a) any deficiencies, failings, or matters requiring attention with respect to the Bank's BSA/AML compliance program identified by any United States regulatory authority within 30 business days of any such regulatory notice; and (b) any steps taken or planned to be taken by USB to address the identified deficiency, failing, or matter requiring attention. The Office may, in its sole discretion, direct USB to provide other reports about its BSA/AML compliance program as warranted.

Limits of this Agreement

22. It is understood that this Agreement is binding on the Office but does not bind any other Federal agencies, any state or local law enforcement agencies, any licensing authorities, or any regulatory authorities. However, if requested by USB or its attorneys, the Office will bring to the attention of any such agencies, including but not limited to any regulators, as applicable, this Agreement, the nature and quality of USB's cooperation, and USB's compliance with its obligations under this Agreement.

Sale or Merger of USB

23. Except as may otherwise be agreed by the parties hereto in connection with a particular transaction, USB agrees that in the event it sells, merges, or transfers all or substantially all of its business operations as they exist as of the date of this Agreement, whether such sale is structured as a sale, asset sale, merger, or transfer, it shall include in any contract for sale, merger or transfer a provision binding the purchaser, or any successor in interest thereto, to the obligations described in this Agreement.

Public Filing

24. USB and the Office agree that, upon the submission of this Agreement (including the Statement of Facts and other attachments hereto) to the Court, this Agreement (and its attachments) shall be filed publicly in the proceedings in the United States District Court for the Southern District of New York.

25. The parties understand that this Agreement reflects the unique facts of this case and is not intended as precedent for other cases.

Execution in Counterparts

26. This Agreement may be executed in one or more counterparts, each of which shall be considered effective as an original signature. Further, all digital images of signatures shall be treated as originals for all purposes.

Boyd M. Johnson, Esq.
Samuel W. Seymour, Esq.
February 12, 2018

Integration Clause

27. This Agreement sets forth all the terms of the Deferred Prosecution Agreement between USB and the Office. No modifications or additions to this Agreement shall be valid unless they are in writing and signed by the Office, USB's attorneys, and a duly authorized representative of USB.

GEOFFREY S. BERMAN
United States Attorney
Southern District of New York

/s/ NIKETH VELAMOOR
By: /s/ JONATHAN COHEN
NIKETH VELAMOOR
JONATHAN COHEN
Assistant United States Attorneys

/s/ ROBERT KHUZAMI
ROBERT KHUZAMI
Deputy United States Attorney

Accepted and agreed to:

/s/ JAMES L. CHOSY — 2/13/2018
JAMES L. CHOSY — Date
Exec. V.P. and General Counsel, U.S. Bancorp

/s/ BOYD M. JOHNSON III, ESQ. — 2/13/2018
BOYD M. JOHNSON III, ESQ. — Date
Wilmer Hale LLP
Attorney for U.S. Bancorp

/s/ SAMUEL W. SEYMOUR, ESQ. — 2/13/2018
SAMUEL W. SEYMOUR, ESQ. — Date
Sullivan & Cromwell LLP
Attorney for U.S. Bancorp

Exhibit A

U.S. BANCORP

CERTIFICATE OF CORPORATE SECRETARY

I, Laura Bednarksi, do hereby certify that I am the duly elected and acting Corporte Secretary of U.S. Bancorp, a Delaware corporation. I further certify that attached hereto as Exhibit A is a true, correct and complete copy of a resolution adopted by the Company's Board of Directors at a meeting duly called and held on February 13, 2018.

IN WITNESS WHEREOF, I have hereunto signed my name effective as of this 13th day of February, 2018.

(No corporate seal)

/s/ Laura F. Bednarski
Laura F. Bednarski
Corporate Secretary

RESOLUTIONS OF THE
BOARD OF DIRECTORS OF
U.S. BANCORP

February 13, 2018

WHEREAS, U.S. Bancorp (the "Company"), together with its legal counsel, has been in discussions with the U.S. Attorney's Office for the Southern District of New York (the "U.S. Attorney's Office") regarding the resolution of an investigation (the "DOJ Investigation") being conducted by the U.S. Attorney's Office regarding (i) a legacy relationship between U.S. Bank National Association ("U.S. Bank") and payday lending businesses associated with former customer Scott Tucker and (ii) U.S. Bank's legacy Bank Secrecy Act/anti-money laundering compliance program, including through the entry by the Company into a Deferred Prosecution Agreement with the U.S. Attorney's Office, substantially in the form that was provided to the Board of Directors of the Company (the "Board") on the date hereof (the "Agreement"); and

WHEREAS, the Company, together with its legal counsel, has also been in discussions with the (i) Office of the Comptroller of the Currency (the "OCC") and the Financial Crimes Enforcement Network ("FinCEN") regarding the resolutions of their reviews (the "OCC Review" and the "FinCEN Investigation," respectively) of U.S. Bank's legacy Bank Secrecy Act/anti-money laundering compliance program and (ii) the Board of Governors of the Federal Reserve System (the "Federal Reserve") regarding the resolution of its review (the "Federal Reserve Review") of the Company's firmwide Bank Secrecy Act/anti-money laundering compliance program and sanctions compliance program,; and

WHEREAS, the Company's General Counsel, James L. Chosy, together with outside counsel for the Company, have advised the Board of the terms of the Agreement and the consequences of entering into (i) the Agreement and all other settlement documentation with the U.S. Attorney's Office, (ii) the Consent Order for a Civil Money Penalty to be issued to U.S. Bank by the OCC (the "OCC Consent Order") and all other settlement documentation with the OCC, (iii) the Stipulation of Settlement and Order of Dismissal, Consent Judgment, and Assessment of Civil Money Penalty to be entered into by U.S. Bank and FinCEN (the "FinCEN Stipulation") and all other settlement documentation with FinCEN and (iv) the Order to Cease and Desist and Order of Assessment of a Civil Money Penalty Issued Upon Consent Pursuant to the Federal Deposit Insurance Act, as Amended, to be entered into among the Company, USB Americas Holding Company and the Federal Reserve (the "Federal Reserve Order") and all other settlement documentation with the Federal Reserve; and

WHEREAS, the Board has determined that it is in the best interests of the Company and U.S. Bank (i) for the Company to enter into the Agreement and for the Company and U.S. Bank, each to the extent necessary, to enter into any other settlement agreements and documents with the U.S. Attorney's Office to resolve the DOJ Investigation, (ii) for U.S. Bank to enter into a Stipulation and Consent to the Issuance of an Order for a Civil Money Penalty (the "OCC Stipulation") and for the Company and U.S. Bank, each to the extent necessary, to enter into any other settlement agreements and documents with the OCC to resolve the OCC Review, (iii) for U.S. Bank to enter into the FinCEN Stipulation, and for the Company and U.S. Bank, each to the extent necessary, to enter into any other settlement agreements and documents with FinCEN to

resolve the FinCEN Investigation and (iv) for the Company and USB Americas Holding Company to enter into the Federal Reserve Order and for the Company and U.S. Bank, each to the extent necessary, to enter into any other settlement agreements and documents with the Federal Reserve to resolve the Federal Reserve Investigation; and

NOW, THEREFORE BE IT RESOLVED, that the Board hereby approves the Agreement, with such changes as James L. Chosy or Andrew Cecere, President and Chief Executive Officer (each, an "Authorized Officer") may approve, and any other settlement agreements and documents with the U.S. Attorney's Office in connection with the DOJ Investigation and authorizes (i) the Authorized Officers and outside counsel representing the Company to execute and deliver the Agreement on behalf of the Company and for them, with such changes as the Authorized Officers and outside counsel may approve, (ii) the Authorized Officers to execute and deliver any and all other agreements and documents necessary to settle the DOJ Investigation, (iii) Michael Greenman, or any other appropriate officer of the Company, to take all actions as in his judgment shall be necessary, appropriate or advisable to carry out the intent and purpose of the Agreement and any and all other agreements and documents necessary to settle the DOJ Investigation and (iv) the Company to perform its obligations under the Agreement and any other settlement agreements and documents with the U.S. Attorney's Office in all respects, including the payment of a money penalty totaling $528,000,000, a portion of which shall be credited for the amount of the civil money penalty paid to the OCC, for a net payment to the U.S. Attorney's Office totaling $453,000,000; and further

RESOLVED, that the Board hereby approves the OCC Stipulation, substantially in the form provided to the Board on the date hereof, with such changes as the Authorized Officers may approve, and any other settlement agreements and documents with the OCC in connection with the OCC Review and authorizes (i) the Authorized Officers, to the extent necessary, to execute and deliver any and all agreements and documents necessary to settle the OCC Review, and (ii) U.S. Bank to perform its obligations under the OCC Consent Order, OCC Stipulation and any other settlement agreements and documents with the OCC in all respects, including the payment of the civil money penalty against U.S. Bank totaling $75,000,000; and further

RESOLVED, that the Board hereby approves the entry by the U.S. Bank into the FinCEN Stipulation, substantially in the form provided to the Board on the date hereof, with such changes as the Authorized Officers may approve, and any other settlement agreements and documents with FinCEN in connection with the FinCEN Investigation, in each case, as approved by the Authorized Officers, and authorizes (i) the Authorized Officers, to the extent necessary, to execute and deliver any and all agreements and documents necessary to settle the FinCEN Investigation and (ii) U.S. Bank to perform its obligations under the FinCEN Stipulation and any other settlement agreements and documents with FinCEN in all respects, including the payment of the civil money penalty totaling $185,000,000, a portion of which shall be credited for a portion of the money penalty paid to the U.S. Attorney's Office, for a net payment to FinCEN totaling $70,000,000; and further

RESOLVED, that the Board hereby approves the entry by the Company into the Federal Reserve Order, with such changes as the Authorized Officers may approve, and any other settlement agreements and documents with the Federal Reserve in connection with the Federal Reserve Review, in each case, as approved by the Authorized Officers, and authorizes (i) the

Authorized Officers to execute and deliver the Federal Reserve Order and any and all other agreements and documents necessary to settle the Federal Reserve Review, (ii) the Company to perform its obligations under the Federal Reserve Order and any other settlement agreements and documents with the Federal Reserve in all respects, including the payment of the civil money penalty totaling $15,000,000; and further

RESOLVED, that the Authorized Officers and such persons as they respectively designate in writing are each authorized, in the name and on behalf of the Company and U.S. Bank, to take or cause to be taken any and all further actions, and to prepare, execute and deliver any and all further agreements, instruments, documents, certificates and filings, and to incur and pay all such fees, commissions and expenses as in the judgment of either of them shall be necessary, appropriate or advisable to carry out the intent and purpose of the foregoing resolutions; and further

RESOLVED, that the necessity, advisability and appropriateness of any action taken, any approval given or any amendment or change to any document or agreement made by any Authorized Officer pursuant to the authority granted under these resolutions shall be conclusively evidenced by the taking of any such action, or the execution, delivery or filing of any such document or agreement; and further

RESOLVED, that any and all actions heretofore taken by any Authorized Officer, or those acting at the direction of either of them, in connection with any matters referred to or contemplated by any of the foregoing resolutions are hereby approved, ratified and confirmed in all respects.

Exhibit B

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA - v. - U.S. BANCORP, Defendant.	INFORMATION 18 Cr.

COUNT ONE
(Willful Failure to Maintain an Adequate Anti-Money Laundering Program In Violation of the Bank Secrecy Act)

The United States Attorney charges:

1. From at least in or about 2009 through in or about 2014, in the Southern District of New York and elsewhere, U.S. Bancorp ("USB"), the defendant, through its subsidiary, U.S. Bank National Association (the "Bank"), did willfully fail to establish, implement, and maintain an adequate anti-money laundering program, to wit, USB did, among other things, cap the number of alerts generated by its transaction monitoring systems based on staffing levels and resources and fail to monitor non-customer Western Union transactions at branches of the Bank, which resulted in a failure to monitor, investigate, and report substantial numbers of suspicious transactions flowing through the Bank.

(Title 31, United States Code, Sections 5318(h), 5322(a) and (c); and
Title 31, Code of Federal Regulations, Section 1020.210.)

COUNT TWO
(Willful Failure to File a Suspicious Activity Report In Violation of the Bank Secrecy Act)

The United States Attorney further charges:

2. From in or about October 2011 through in or about November 2013, in the Southern District of New York and elsewhere, USB, the defendant, through the Bank, did willfully fail to report suspicious transactions relevant to a possible violation of law or regulations, as required by the Secretary of the Treasury, to wit, USB willfully failed to timely report suspicious banking activities of Scott Tucker, a customer, who used the Bank to launder proceeds from an illegal payday lending scheme.

(Title 31, United States Code, Sections 5318(g), 5322(a) and (c); and
Title 31, Code of Federal Regulations, Section 1020.320.)

/s/ GEOFFREY S. BERMAN
GEOFFREY S. BERMAN
United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

U.S. BANCORP,
Defendant.

INFORMATION

18 Cr.

(18 U.S.C. §§ 5318 and 5322;
31 C.F.R. §§ 1010.210 and 1020.320)

GEOFFREY S. BERMAN
United States Attorney.

Exhibit C

INTRODUCTION

1. The following Statement of Facts is incorporated by reference as part of the deferred prosecution agreement (the "Agreement") between the United States Attorney's Office for the Southern District of New York (the "Office") and U.S. Bancorp.

2. The parties agree and stipulate that the information contained in this Statement of Facts is true and accurate.

OVERVIEW

3. U.S. Bancorp is a bank holding company based in Minneapolis, Minnesota. It is listed on the New York Stock Exchange. U.S. Bancorp's subsidiary U.S. Bank National Association ("USB" or the "Bank") is the fifth largest bank in the United States. Headquartered in Minneapolis, Minnesota, the Bank has over 3,100 branches. Throughout the relevant time period, USB's banking activity was predominantly retail and almost entirely domestic.

4. The Office has alleged, and U.S. Bancorp accepts, that its conduct through USB, as described herein, violated Title 31, United States Code, Sections 5318(g), 5318(h) and 5322(a)-(c) because USB willfully (i) failed to maintain an adequate anti-money laundering ("AML") program and (ii) failed to report suspicious transactions relevant to a possible violation of law or regulations as required by the Secretary of the Treasury.

5. From at least in or about 2009, and continuing until 2014, USB willfully failed to establish, implement and maintain an adequate AML program. Among other things, USB capped the number of alerts generated by its transaction monitoring systems based on staffing levels and resources and failed to monitor non-customer Western Union transactions at branches of the Bank, which resulted in the Bank failing to monitor, investigate and report substantial numbers of suspicious transactions flowing through the Bank. The Bank's then Chief Compliance Officer concealed the Bank's practices from the Office of the Comptroller of the Currency ("OCC"), the Bank's primary regulator.

6. In separate but related conduct, from at least in or about October 2011 through in or about November 2013, the Bank willfully failed to timely report suspicious banking activities of Scott Tucker, its longtime customer, despite being on notice of facts giving rise to suspicion that Tucker had used and was using the Bank to launder more than two billion dollars of proceeds from an illegal payday lending scheme.

THE BANK SECRECY ACT'S REQUIREMENTS

7. The Currency and Foreign Transactions Reporting Act of 1970 (commonly known as the Bank Secrecy Act or BSA), Title 31, United States Code, Section 5311, *et seq.*, requires financial institutions – including USB – to take certain steps to protect against their use to commit crimes and launder money.

8. The BSA requires financial institutions to establish and maintain adequate AML compliance programs that, at a minimum and among other things, comprise the following: (a) internal policies, procedures, and controls designed to guard against money laundering; (b) an individual or individuals to coordinate and monitor day-to-day compliance with BSA and AML requirements; (c) an ongoing employee training program; and (d) an independent audit function to test compliance programs. 31 U.S.C. § 5318(h).

9. In order to be effective, a bank's AML compliance program must be risk-based and its systems for identifying suspicious activity must be tailored to the bank's risk profile. To that end, management should review and test alert thresholds to ensure that they are appropriate for a bank's risk profile and document how filtering criteria and thresholds used are appropriate for the bank's risks. The systems' programming methodology and effectiveness should be

independently validated to ensure that the models are detecting potentially suspicious activity. The bank must assign adequate staff to the identification, evaluation, and reporting of potentially suspicious activities, taking into account the bank's overall risk profile and the volume of transactions.

10. Regulatory guidance in effect during the relevant time period provided that the cornerstone of a strong AML program is the adoption and implementation of comprehensive customer due diligence ("CDD") policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering. Effective CDD policies, procedures and processes enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage, comply with regulatory requirements and report suspicious activity. CDD begins with verifying the customer's identity. Accordingly, regulations in effect during the relevant time period also required that AML programs implement a Customer Identification Program ("CIP"), which must include reasonable and practicable risk-based procedures for verifying the true identity of the bank's customers and the nature of their businesses and activities.

11. The BSA and regulations issued under the BSA in effect during the relevant time period required financial institutions to report "suspicious transaction[s] relevant to a possible violation of law or regulation." 31 U.S.C. § 5318(g)(1); 31 C.F.R. § 1020.320(a)(1). BSA regulations provide that a transaction is reportable if it is "conducted or attempted by, at, or through the bank," "involves or aggregates at least $5,000 in funds or other assets," and "the bank knows, suspects, or has reason to suspect that . . . [t]he transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source,

location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation" or that the "transaction has no business or apparent lawful purpose." 31 C.F.R. § 1020.320(a)(2). Financial institutions satisfy their obligation to report such a transaction by filing a suspicious activity report ("SAR") with the Financial Crimes Enforcement Network ("FinCEN"), a part of the United States Department of the Treasury. 31 C.F.R. § 1020.320(b).

USB'S FAILURE TO MAINTAIN AN ADEQUATE AML PROGRAM

12. USB's AML compliance department, referred to internally as Corporate AML, had primary responsibility for the Bank's fulfilment of its obligations under the BSA. At all relevant times, Corporate AML was supervised by the Bank's Chief Compliance Officer, who reported to the Chief Risk Officer, who in turn reported to the Chief Executive Officer. USB also had an AML Officer, who reported to the Chief Compliance Officer. In 2007, USB named as Chief Compliance Officer an attorney who had no prior AML experience at USB or elsewhere (the "CCO"). Soon thereafter, the CCO named as AML Officer a lawyer who also had no AML experience (the "AMLO"). Although he was promoted in 2010, the CCO retained oversight over the AML program until 2014.

13. For much of the relevant period, USB had only 25-30 AML investigators. Apart from investigators added as a result of acquiring other banks, USB did not increase substantially its number of investigators. As late as 2012, when USB had over $340 billion in assets, the Bank had 32 investigators. USB also failed to increase salaries of certain AML employees even after Human Resources and Compliance personnel complained to the CCO and the Chief Risk Officer that the Bank was paying its investigators below-market salaries and competitor banks were successfully poaching USB investigators. USB filled key compliance roles, including policy-making and transaction monitoring positions, with individuals who, by their own admission, lacked experience. The compliance department also requested but did not receive adequate funding for computers and other hardware needed to support monitoring systems, and was forced to delay certain upgrades of its systems until 2014, after the versions it was using had become obsolete in the industry.

USB's Capping of SearchSpace Alerts

14. In April 2004, USB began using SearchSpace, a commercially available software system for monitoring transactions flowing through the Bank. The automated monitoring tools that USB ran against the data in SearchSpace were the "Security Blanket" and Queries. The Security Blanket examined transactions that fed into SearchSpace and, on a monthly basis, assigned each transaction a score to reflect the extent to which it was unusual or unexpected for the customer. The Bank began implementing Queries to complement the Security Blanket in 2005. Queries were "rules" that were run against transaction data in SearchSpace to identify indicia of potentially suspicious activity.

15. When it first began using SearchSpace, the Bank, at the recommendation of the SearchSpace vendor, configured the system so that the Security Blanket would generate a fixed number of alerts per month, rather than setting a risk-based threshold that would have generated all alerts naturally occurring at or above the score corresponding to a certain level of risk. USB configured the Security Blanket in this manner until 2013, even after its compliance professionals learned that doing so was inconsistent with industry standards.

16. Over time, even as the Bank grew in size, it reduced the number of Security Blanket alerts that it would review each month from a high of 1,500 in 2004 to 500 by 2009. Decisions to reduce the alert quota were made at "tuning committee" meetings. Minutes of Security Blanket tuning meetings were not kept, while decisions to reduce alert quotas were documented in project memoranda. The rationale in these memoranda for the alert cap reductions was typically the desire to focus investigative resources on Queries, which were more likely than the Security Blanket to detect suspicious activity.

17. However, USB had in place only 22 different Queries and set numerical caps on alerts arising from the six Queries that typically generated the largest volumes of alerts. The rationale for these caps was not reflected in minutes of Query Tuning meetings. For the results of several Queries targeting wire activity, the Bank adopted a "triage" process to decide which alerts to investigate. USB did not have a procedure or policy document in place to explain this process until the OCC asked about it in April 2014. Given the large number of alerts generated and the limitations on investigative resources, this "triage" approach had the practical effect of limiting the number of alerts that were investigated. For example, the wire report for June 2013 showed over 57,000 customers (some of which may be duplicates) alerted for wire activity, but less than 100 of those customers received an investigative review. For the remaining queries, which generally involved the generation of relatively few alerts, the Bank reviewed all of the alerts.

18. Contemporaneous documentation from as early as 2005 acknowledged that the limits on alerts were "increasingly based on staffing levels" and, as a result, constituted a "risk item" for the bank. Requests for additional investigator staffing were made but did not result in any meaningful increase in the number of investigators. In a December 1, 2009 memo from the AMLO to the CCO, the AMLO explained: "As you know, we have been experiencing significant increases in our SAR volumes, query effectiveness, closure recommendations and law enforcement inquiries," but, "[i]n the face of these increases, we have held staffing relatively constant." The memo further explained that the SAR volume for 2009 was projected to be 47% higher than for 2007, law enforcement inquiries were projected to be 123% higher, and closure recommendations were projected to be 160% higher—all with a corresponding staff level increase of only 15.6%. The AMLO noted that this mismatch would generate "increased workload and staff that already is stretched dangerously thin." The AMLO then added:

> The above numbers are especially distressing give[n] the fact that an increase in the number of alerts worked is imminent and necessary. On a monthly basis, Corporate AML tests a small sample of items that fall less than 10% outside the alert threshold in SearchSpace. As of October 2009, Corporate AML had tested 47 such items, 17 of which resulted in a SAR. This is a SAR filing percentage of 26%. . . . A regulator could very easily argue that this testing should lead to an increase in the number of queries worked.

Given this, the AMLO requested an opportunity to meet with the CCO to discuss staff increases. When that request went unanswered, the AMLO followed up with a similar memo on April 23, 2010. In that memo, the AMLO repeated that despite increases in SAR volumes, staffing had remained "relatively constant" and "dangerously thin," and again requested an opportunity to meet with the CCO to discuss staff increases. Several months later, the Bank hired two additional investigators.

19. Meanwhile, in July 2010, AML employees worked to develop a database to track subpoenas, summonses, and other legal process, which, according to an AML Compliance Manager, would "help bring [the Bank] into full compliance with the OCC guidelines requiring reviews of accounts of customers for which we have received a grand jury subpoena." Based on their analysis, these employees expected to receive 340 alerts per month, which would have covered all legal process, including grand jury subpoenas. When they presented their proposal and accompanying expectations to the AMLO, he responded, in part, that "340 new alerts is not practical to take on UNTIL the staff is there to work them." Neither this proposal, nor a more targeted proposal to review accounts for which the Bank received a grand jury subpoena, was implemented at that time.

20. This problem of inadequate staffing persisted at least until 2014. In January 2013, for example, AML employees continued to discuss "AML alert volume vs. staffing levels" and, specifically, "how we move forward with the continuing gap between alert volume and our investigator workforce due to inability to get job offers approved." At the time, the Corporate AML employee who was responsible for managing the SearchSpace system (the "Employee") reported to the Bank's new AML Officer, who joined USB in July 2012, that the "total number of outstanding alerts" had grown significantly since November 1, 2012.

21. Soon after the new AML Officer joined USB, he ordered that the Bank's practice of limiting the number of Security Blanket alerts be halted. In response, in February 2013, the Bank removed the fixed limits from the Security Blanket settings but replaced them with fixed score thresholds chosen to indirectly replicate the limit of 500 alerts previously in place. The Bank then used the same score thresholds from month-to-month, and did not adjust the thresholds based on further risk-based tuning. After moving to this approach, the number of monthly alerts remained roughly constant: approximately 500 per month (ranging from 380 to 610 total alerts). Moreover, even after the new AML Officer directed that limits on Security Blanket alerts be lifted, USB maintained its alert caps on Queries until 2014.

USB's Termination of Below-Threshold Testing Due to Lack of Resources

22. From at least 2007, the Bank conducted below-threshold testing ("BTT") on several Queries to determine if its alert caps were causing the Bank to miss large numbers of suspicious transactions. This involved selecting a sampling of alerts occurring immediately below the alert thresholds – alerts that were not ordinarily being investigated given the thresholds that were in place – and then having investigators review them in order to determine whether the thresholds should be adjusted because suspicious activity was occurring below the threshold.

23. To estimate how much suspicious activity was occurring below the threshold, and therefore not being investigated, the Bank calculated the percentages of the reviewed below- threshold alerts that resulted in the filing of a SAR. The Bank's BTT consistently yielded high ratios of SARs filed to number of alerts tested below the threshold—often well in excess of 25% — that indicated that thresholds should be lowered. In November 2011, the Employee, who was responsible for conducting BTT, informed the AMLO that, "[o]ver the past year, the SAR rates for our below threshold testing has averaged between 30% - 80% for the 4 queries where we perform the testing[,]" where a SAR rate of 80% indicates that the Bank would file SARs on four out of every five additional alerts it chose to investigate. Tuning Committee members wanted to lower the thresholds in order to increase the number of alerts being reviewed, but were unable to do so because the Bank lacked sufficient resources to investigate additional alerts.

24. Rather than increasing resources and adjusting thresholds to ensure that the appropriate volume of potentially suspicious activity was investigated, in or about April 2012, the Bank stopped conducting BTT altogether. The Employee, who was responsible for preparing minutes of tuning committee meetings, included a pretextual explanation for the Bank's decision in the minutes: that a "majority" of the customers whose activity was identified as SAR-worthy during BTT would eventually move above the threshold and become subject to review in the ordinary course. The AML employee who developed this rationale acknowledged to the Employee that it was based on analysis of "a small sample size" that in fact reflected an eventual migration rate to above-threshold of less than 50 percent, and said nothing of the delay in reviewing those accounts that would eventually migrate. The AML employee opined, "I believe we can argue in support of my supposition that over time at least some under threshold customers will move above threshold and be investigated . . . . This could impact the empirical value and review of our current practice to sample below threshold. just sayin."

25. In reality, the primary reason the Bank stopped conducting BTT was that BTT was showing high SAR rates below-the-line, which the Bank was not addressing due to resource limitations. The Employee deliberately did not include that reason in the minutes of the meeting at which BTT was terminated in part because he knew that the OCC, which could request the minutes, would disapprove, and because he wanted to protect himself and his supervisor from adverse consequences.

26. The OCC's primary bank examiner assigned to the Bank's AML program had repeatedly warned certain USB officials, including the AMLO, that managing the Bank's monitoring programs to the size of its staff and other resources would get the Bank in trouble with the OCC. According to tuning committee meeting participants, they discussed the fact that the OCC did not approve of numerical limits and could bring an enforcement action against the Bank on this issue. The AMLO, in his December 1, 2009 memo to the CCO about BTT, reminded the CCO that a "regulator could very easily argue that this testing should lead to an increase in the number of queries worked."

27. Although USB provided documentation to the OCC during reviews in 2008 and 2010 that indicated specific monthly targets for Security Blanket alerts, particular numbers of Query alerts the Bank was working and results of BTT, USB officials failed to disclose the Bank's resource-based alert caps to the OCC, even when asked about the Bank's alert management practices. After USB hired new Chief Compliance and AML Officers (the "New Officers") in 2012, the CCO discouraged them from removing alert threshold limits and disclosing them to the OCC by representing to the New Officers that the OCC was fully aware of

the Bank's monitoring practices and therefore had at least tacitly approved them. According to information gathered by one of the New Officers in 2014, the AMLO had previously answered questions from the OCC examiner assigned to AML without providing direct and meaningful answers. Driven in large measure by instructions from the CCO, compliance employees consistently did not volunteer information to regulators, including deficiencies with the program, except in response to specific requests. In 2013, the AMLO stated to another senior manager at USB that USB's AML program was an effort to use "smoke and mirrors" to "pull the wool over the eyes" of the OCC.

28. In 2013, after the OCC's chief examiner encouraged the Bank's CEO to speak with the New Officers about the AML program, the New Officers prepared a PowerPoint presentation for the CEO that identified multiple vulnerabilities in the Bank's AML program, and explained how those same problems had led the OCC to take action against other banks. The New Officers' draft presentation explicitly referred to various problems with the Bank's AML program, including, among other things, "[m]anipulation of system output through use of alert caps on both profiling and query detection methods" that could "potentially result in missed Suspicious Activity Reports" and "[p]otential regulatory action resulting in fines, consent order, and significant historical review of transactions." The CCO reviewed the draft and removed references to alert caps from the presentation, added positive information about the Bank's AML program, and otherwise altered the deck to present a more favorable image of the Bank's AML program.

29. USB also failed to have SearchSpace independently validated in accordance with regulatory guidance, which the OCC recommended to USB as early as 2008. The Bank completed a validation after that recommendation and prior to the OCC's review of SearchSpace in 2010, but the OCC informed the Bank that its validation was not performed independently and expressly recommended that the Bank complete an independent validation. In lieu of independent validation, as late as 2013, the Employee, who was responsible for managing the SearchSpace system, prepared a "biannual SearchSpace Model validation" and asked another Bank employee to review it and acknowledge having done so, while assuring him that he was "not making any representation that you are validating anything." The Employee acknowledged that the regulator "could (and probably will at some point), force us to hire outside auditors to perform a more robust independent validation/review" but stated that "this would cost tens of thousands . . . minimum. Until we are forced to go there . . . you are sufficient." The Bank justified its failure to conduct an independent validation to the OCC by claiming that it was planning an upgrade of its transaction monitoring system from SearchSpace to a more advanced program. In reality, that upgrade did not occur until 2014.

USB'S Failure To Monitor Western Union Transactions

30. In May 2009, USB began offering both customers and non-customers the ability to conduct Western Union ("WU") currency transactions at USB branches. In 2012, the Bank handled 1.1 million WU transactions totaling $582 million, approximately half of which were from non-customers. As the company recognized in internal documents, the WU money transfer was one of the highest risk products that the Bank offered. According to an internal summary of WU transactions in 2013, over 40 per cent of the total number of WU wires flowing through the Bank and over 50 per cent of the total wire amounts involved countries on the Bank's Primary or Secondary High-Risk Country lists, including Nigeria, Pakistan, Colombia, Afghanistan and Lebanon.

31. At the beginning of its relationship with WU, no one at the Bank performed an initial risk assessment or systematically reviewed the total suspicious activity involving WU transactions to determine if WU itself was a higher-risk customer. The Bank's contract with WU required WU to have an AML program in place to detect and report suspicious activity, but USB employees, including the CCO and AMLO, were aware that, under applicable regulatory guidance, the Bank's AML requirements applied to WU transactions conducted at Bank branches. They also knew that WU transactions not processed through an account of the Bank (that is, WU transactions involving non-customers of the Bank) would not be monitored in SearchSpace. Nonetheless, USB went forward with processing WU transactions involving non- customers even though they would not be subject to transaction monitoring.

32. When Bank employees flagged transactions involving non-customers by filling out Internal Referral Forms ("IRFs"), IRFs raising fraud concerns were investigated by the Corporate Security department but IRFs raising AML-related concerns went uninvestigated. In a December 2011 internal email, an employee in Corporate Security stated that "[a]ccording to the OCC, regardless if they are a customer or not, if we (US Bank) are notified of the suspicious activity, we are liable if we do not file a SAR if it is required . . . ." Thereafter, AML-related IRFs were forwarded to Corporate AML for investigation, but Corporate AML did not begin to investigate these IRFs until June 2013.

33. In mid-2012, Corporate AML became aware of a criminal investigation of WU. In or about June 2012, the Bank began to take steps to address gaps in its monitoring of WU transactions, but the steps were limited. In December 2012, the new AML Officer emailed the CCO with concerns about WU monitoring. In response, the CCO dismissed the new AML Officer's concerns and chastised him for recording them in an email. During 2013, the Bank

filed approximately seven SARs per month on WU activity but failed to increase its reviews due to staffing issues. Finally, on July 1, 2014, the Bank implemented a policy requiring that all WU transactions conducted at Bank locations be done through an account of a Bank customer—a policy that foreclosed Bank processing of WU transactions by non-customers.

OCC Investigation And Consent Order

34. In or around February 2014, the OCC's then-new examiner responsible for the Bank's AML program, who had previously worked at the Bank, found evidence that the Bank was restricting the volume of alerts that it was investigating and began to question the Bank's alert management processes. For several months following these initial inquiries, certain USB personnel who were aware of the Bank's resource-driven alert management practices, including the CCO, did not fully disclose them to OCC personnel. Eventually, the new AMLO elevated his concerns to USB's newly-appointed Chief Risk Officer (the "CRO"), informing him that, contrary to what he had previously been led by the CCO to believe, the OCC had not been aware of the Bank's alert management practices. Meanwhile, after growing frustrated with their ability to get straight answers to their questions from Bank personnel, particularly the CCO, the OCC elevated its concerns to the new CRO.

35. In or about June 2014, the CRO caused the Bank to retain outside counsel to conduct an internal review of the Bank's alert management practices and monitoring of Western Union transactions. The CCO was removed from having oversight over Corporate AML and offered a lesser position but left the Bank. The AMLO, who had been replaced by the new AMLO in 2012, left the Bank in 2014. The Employee was terminated in 2015.

36. In November 2014, outside counsel reported the results of the review to the OCC. In October 2015, the Bank entered into a consent order with the OCC based on various deficiencies in its AML compliance program, including gaps in suspicious activity monitoring, insufficient staffing and inadequate monitoring of Western Union transactions.

37. Pursuant to the consent order, the Bank performed a look-back analysis to assess the impact of the Bank's deficient monitoring practices. Specifically, the Bank reanalyzed transactions that occurred during the six months prior to taking steps to remedy these practices, including removing fixed limits on Security Blanket alerts, lifting caps on and expanding coverage of various Queries, and excluding non-customers from WU. The look-back analysis resulted in the generation of an additional 24,179 alerts and the filing of 2,121 SARs. The value of the transactions reported in these SARs was $719,465,772.

38. Since 2015, USB has replaced Corporate AML with a new department called Enterprise Financial Crimes Compliance and spent more than $200 million in enhancements to its AML program, including software, technology and increased staffing. USB replaced SearchSpace with a new transaction monitoring program and developed and deployed a new transaction monitoring strategy. The Bank increased its AML and related compliance staff by 156% and now employs 540 fulltime employees, including 228 AML individuals whose responsibilities include investigating suspicious activity alerts.

USB's FAILURE TO TIMELY FILE SUSPICIOUS ACTIVITY REPORTS RELATING TO SCOTT TUCKER

39. On October 13, 2017, Scott Tucker ("Tucker") and his attorney, Timothy Muir, were convicted in the United District Court for the Southern District of New York of racketeering, wire fraud and money laundering for their roles in perpetrating a massive payday lending scheme. From in or about the late 1990s through in or about 2013, through various companies that he owned and controlled (the "Tucker Payday Lenders"), Tucker extended short- term, high-interest, unsecured loans, commonly referred to as "payday loans," to individuals in

New York and around the country at interest rates as high as 700 percent or more and in violation of the usury laws of numerous states, including New York. Tucker sought to evade applicable laws by entering into a series of sham relationships with certain Native American tribes (the "Tribes") in which he assigned nominal ownership of his payday lending companies to certain corporations created under the laws of the Tribes (the "Tribal Companies") in order to conceal his ownership and control of the Tucker Payday Lenders and gain the protection of tribal sovereign immunity—a legal doctrine that generally prevents states from enforcing their laws against Native American tribes. On February 10, 2016, the Office entered into a nonprosecution agreement with certain Tribal Companies pursuant to which the Tribal Companies agreed to forfeit $48 million in criminal proceeds from the Tucker Payday Lenders.

40. Tucker began banking with institutions later acquired by USB in September 1997, and continued to open new accounts with USB through 2013. Tucker opened and maintained numerous operating accounts in the names of the Tribal Companies as well as accounts in the names of other companies that he owned and controlled. For the vast majority of payday loan transactions with individual borrowers, the Tucker Payday Lenders relied on payment processors, which utilized banks other than USB to serve as the Originating Depository Financial Institution ("ODFI") to credit and debit the borrowers' bank accounts. The Tucker Payday Lenders used operating accounts at USB to send daily wire transfers to, and receive daily wire transfers from, these payment processors for these transactions. Operating accounts at USB were also used to pay other expenses of the business, including lead generation and advertising expenses. Given the size of the payday loan business, these accounts fell under the administration of the Bank's Middle Market Commercial Banking group. From 2008 through 2012, the Tucker Payday Lenders extended approximately 5 million loans to customers across the country, while generating more than $2 billion dollars in revenues and hundreds of millions of dollars in profits. Most of this money flowed through accounts that Tucker had opened at USB.

41. From 2002 until 2010, the Bank's relationship with Tucker and the accounts he opened was managed by a relationship manager based in the Kansas City area (the "RM"). USB's policies provided, consistent with applicable regulations, that whenever it opened an account for a new customer, including "the first time a TIN is entered on an application system[,]" commercial bankers were required to "[i]nterview the customer to fully understand the nature of the client's ownership, business and sources of income" and "[u]nderstand the types of activities that will be transacted with the Bank and the client's 'normal' transaction patterns, especially related to cash activity, wire transfers and foreign or offshore transactions."

42. Although most of the new accounts Tucker opened were in the names of entities with TINs as yet unassociated with any existing account at the Bank, the Bank made little effort to understand the activities of these entities or their ownership, or to conduct meaningful due diligence on Tucker or his payday lending business. Several bank employees involved in the Tucker accounts, including the RM, did not accurately understand which customer entities were (nominally) owned by the Tribes and which were owned by Tucker and/or his brother, who was Tucker's sometime business associate, and were not aware of the positions that Tucker and/or his brother held within the Tribal Companies, if any.

43. Consistent with the Bank's CDD policies and as reflected in contemporaneous internal records, the Bank recognized that the accounts Tucker opened in the names of Tribal Companies to facilitate his payday lending business were high risk, and should therefore be subjected to enhanced due diligence. This involved periodic examination of the activity in the accounts to see if it was consistent with expected activity for a payday lender, periodic site visits to ensure the business did what it purported to do, and periodic questionnaires directed at the subject entities.

44. Information obtained by USB in conducting this due diligence included indications suggesting that Tucker was using the Tribes to conceal his ownership and control of the Tucker Payday Lenders. For site visits, Bank employees traveled to Tucker's offices in Overland Park, Kansas, even though the purported customers' addresses—and the only ones listed on the site visit verification forms and questionnaires directed at the Tribal Companies— were those of the Tribes. Although the questionnaires called for disclosure of all addresses and officers of the businesses, USB repeatedly accepted completed questionnaires that omitted Tucker and the Overland Park address and listed instead a single tribal official whom no Bank employee had met—let alone interviewed—and an address that no Bank employee had visited.

45. Some of the documentation that USB accepted as supposed verification that the Tribes were bona fide owners of the Tribal Companies contained indicators that suggested they were not. Tucker opened accounts in the names of numerous different Tribes, including in some cases accounts for multiple Tribes for the same Tucker Payday Lender. The Bank relied in part on Articles of Incorporation and AML policies provided by Tucker and his employees that were ostensibly from different Tribes but that were identical to each other except for the name of the Tribe, as well as business license certificates ostensibly from different Tribes that bore identical fonts, language, and slogans. The Bank also accepted Special Powers of Attorney executed by tribal officials that granted Tucker and certain of his preexisting corporate entities the authority to open and maintain bank accounts on behalf of the Tribal Companies. In approximately the same timeframe, Tucker provided the Bank with multiple signed Corporate Certificate of

Authority documents, the Bank's rough equivalent of signature cards, in which Tucker falsely claimed that he was a Secretary of certain of the Tribal Companies and, on that basis, was an authorized signer of nominally tribal accounts at the Bank. The Bank's diligence procedures did not detect these false statements. No Bank employee ever asked to speak with any of the tribal officials who, according to the CIP/KYC paperwork the Bank routinely accepted from Tucker, purportedly controlled the funds in the Tribal Companies' accounts.

46. USB employees responsible for servicing Tucker's ongoing account activity were also aware of red flags that Tucker was using the Tribes to conceal his ownership and control of the accounts. The Bank's sole points of contact for all the accounts, including the accounts for the Tribal Companies, were some combination of Tucker, his brother, and/or one of their employees in Overland Park, Kansas. In one email from Tucker to the RM, Tucker stated that he was "sensitive" about revealing financial information about himself, as Tucker and the RM had "discussed numerous times." None of the Bank employees had any dealings with any of the tribal officials whose names appeared on some of the account documentation, and, from time to time, heeded Tucker's requests to close accounts purportedly held by Tribal Companies without consulting the tribal officials supposedly associated with those businesses. Tucker also requested that all bank statements for the Tribal Companies' accounts be "held somewhere locally" and/or have a "specific mail address for all account statements to be mailed to that is different than listed on the account." One Bank employee recalled Tucker's brother requesting on two or three occasions that accounts be opened in time to receive incoming wires of less than $10,000 the following day. When that employee raised her concerns about the Tuckers to her supervisors, she was told that the Tuckers were "okay guys" and her concerns were dismissed.

47. Tucker spent large sums of money from the Tribal Companies' accounts on personal items, including tens of millions of dollars on a vacation home in Aspen and the expenses of Tucker's professional Ferrari racing team, which the RM was familiar with in part because he attended at least one race as Tucker's guest. In some instances, Tucker concealed the source of funds by routing payments for these personal expenses, including vehicles, from Tribal Companies' accounts through other USB accounts he owned and controlled before he made final payment to the vendor. Checks for many of the personal expenses were signed using a stamp with the signature of the nominal CEO of certain of the Tribal Companies. In some instances, USB officials were notified of the payments in advance so that they could ensure that they were processed. For example, in 2009, the RM wrote a reference letter on Tucker's behalf to help Tucker purchase the Aspen home. In March 2010, Tucker gave the RM advance notice of a $10 million wire from a bank account nominally belonging to a Tribal Company to Tucker's former business partner towards a settlement of a lawsuit brought against Tucker by the business partner. In September 2010, the RM and another Bank employee assisted the Tuckers with an additional $5 million wire from the same account for the same purpose.

48. During the relevant period, the Bank received subpoenas for bank records from regulators, including the FTC, that had taken or were contemplating enforcement actions against Tucker's businesses. In or about February 2009, the Bank received a subpoena from the State of California. As discussed in court papers received by the Bank, the State served the subpoena to explore its allegation that Tucker's relationship with the Tribes was a sham. Following receipt of the subpoena, the RM met with Tucker and his lawyers to discuss the case and Tucker's motion to quash the subpoena. Per the Bank's practice, it did not provide documents in response to the subpoena while Tucker's motion to quash was pending. When the California court granted the

motion to quash, the RM emailed Tucker to congratulate him. Later, when the States obtained Bank records from the FTC, Bank employees assisted Tucker's lawyers, who were challenging how the States had obtained the records. The receipt of these subpoenas from state and federal regulators and related events did not prompt any investigation by the Bank's AML department.

49. When the RM wrote reference letters for Tucker, including a letter to help Tucker purchase the vacation home discussed above, he claimed that "Tucker and his companies," as of May 1, 2009, "carried in excess of a Mid-Eight Figure average daily collected balance" at the Bank—a ballpark figure that necessarily counted funds in accounts purportedly belonging to the Tribal Companies. In February 2011, the RM became aware of a *Wall Street Journal* article about various payday lenders, including Tucker, who used tribes. The article questioned the legitimacy of these tribal relationships, and quoted one of the officials from a Tribe associated with Tucker saying, when asked where the operation was located, that it was "somewhere in Kansas." The RM emailed the article to Tucker because the RM was "interested in getting your feedback in the event we have people within the bank that ask about it."

50. Throughout the relevant period, Tucker was one of the top two customers in the Bank's Kansas City market, and Bank employees actively pursued and received additional business from him relating to his other business ventures. The Kansas City market brought in approximately $20-$30 million in profit in 2011, and Tucker's accounts comprised 10 percent of that amount. Bank officials described Tucker as the "largest [Treasury Management] customer in the K.C. market" and detailed efforts to "deepen" its relationship with him. In one email in 2007, the RM thanked Tucker for "always giv[ing] [the Bank] an opportunity to be the first to look at anything you are involved in." And throughout the relevant time period, Tucker opened additional accounts and utilized the Bank's services for other opportunities.

51. In April 2011, an account associated with Tucker's brother alerted in SearchSpace for a series of cash withdrawals and an AML analyst (the "Analyst") conducted a review of account activity. The Analyst found that, during the approximately three months surrounding the alert, the account had received checks from one company owned by the brother, a $400,000 distribution payment from another company owned by the brother, and a series of $50,000 payments from the accounts of the Tucker Payday Lenders. During the same period, the Analyst found 17 withdrawals ranging from $1,072.35 to $250,000.00, with the latter being a transfer withdrawal to one of Tucker's brother's companies' accounts.

52. On May 27, 2011, the Analyst requested a Customer Transaction Assessment ("CTA"), seeking additional information about these transactions. A CTA involves sending a form to the banker with a series of questions. The form notes that further explanation is required "to understand transactions which may appear to be suspicious or 'high-risk' for money laundering and is needed to fulfill [the Bank's] regulatory responsibility to document our customer's transaction activity based on *Know Your Customer* requirements and normal and expected account activity." The Analyst's CTA summarized the alerted transactions and other activity and asked specific questions about the customer's business. It also asked specific questions about the purpose of particular transactions that had been identified. The Analyst sent the CTA to the branch associated with the account and set a deadline of June 2, 2011.

53. No one from the branch responded within the requested timeframe, and on the due date, an automated reminder was sent noting that a response was due. A branch employee responded by email the same day that, although he understood his response was overdue, he "really wanted to look into the relationship a bit more before I contacted this client." The employee further stated that the account that a "majority of the funds were transferred to is a

business account with over $2.5 million in it currently and had an avg balance of over $500K last year. I believe that the activity on his personal account was actually for the business, hence the reason most of the funds were transferred directly into that account." The employee expressed that he was "hesitant to contact this customer due to the valuable relationship and I would hate to risk it." The branch employee requested the Analyst's guidance on how to proceed.

54. On June 6, 2011, the Analyst transferred the CTA to the Wholesale Banking and Commercial Relationship division. Prior to receiving a response, and with the 30-day deadline approaching, the Analyst closed the alert without filing a SAR. On June 7, 2011, the CTA was directed to the RM, who responded the same day. The RM stated that "[w]e can find out the answers to some of the questions if you want us to contact [the Tuckers] directly" while also repeatedly citing the Bank's lengthy business relationship with the Tuckers, offering basic information about the nature of the Tuckers' businesses, and claiming that the entirety of the Bank's relationship with Tucker and his brother was "track[ed]" in "the AML group." The RM did not provide any explanation for the cash transactions that had generated the alert, and neither Tucker was contacted for this information.

55. In September 2011, the Center for Public Integrity published a two-part report examining Tucker's history, business practices, and his relationship with the Tribes, and CBS News broadcast an investigative report on Tucker. The report described evidence that the Tribes' relationship to the Tucker Payday Lenders was a sham, explained Tucker's use of shell companies, including many of the companies that had had accounts at the Bank for years, and suggested that Tucker's companies (and possibly Tucker himself) had filed an affidavit with a forged signature in an enforcement action brought by a state regulator. The report also recounted negative information about Tucker's personal history, including allegations that he had made false statements in a bankruptcy and had prior federal criminal convictions, including for an investment fraud scheme in which he had falsely held himself out as a representative of an investment bank.

56. Following the publication of these reports, the RM prepared a memorandum entitled "Situation Overview-Scott Tucker" and sent it to the Kansas City market president and an employee in Wholesale Banking Risk Management ("WBRM") who assessed AML risk. In the memorandum, the RM stated that the reports, to which he provided links, provided a "better understanding of some of the legal issues around the industry but also brought to light some additional information that we were previously unaware of about Scott Tucker" including "[m]ost concerning[,] . . . a federal conviction approximately 20 years ago in which he was sentenced to a year in prison; also, he filed for bankruptcy in 1997." The RM further noted:

> This is a very large TM [Treasury Management] and Deposit relationship in the bank and because of the industry is also considered a high risk for AML purposes . . . . However even with the added due diligence from AML and the Patriot Act, we still did not have any knowledge of the issues surrounding Scott personally. In light of these articles and the fact that one of them references US Bank (relating to a signature card), we have requested a meeting as soon as possible to discuss next steps.

The RM also proposed a series of discussion topics, including whether it was the "recommendation of the [business] line that we exit this relationship, assuming the findings are accurate."

57. Shortly thereafter, the WBRM employee, who had been working with the RM to prepare information about the Tucker relationship for management, made a "Request for Investigation support" to Corporate AML. The WBRM employee stated that "[o]ne of our very large Payday lending key principals has been the key topic of a rather negative investigative news article this week (I Watch News/CBS News)." Attaching the "Situation Overview-Scott Tucker" and pasting a link to the article, the employee explained that the article goes "into the

specifics on a Scott Tucker" including "a criminal record that we want/need some validation" and a claim that "he has pleaded guilty to charges in Federal court and served time in Leavenworth . . . in 1991." The employee further noted that this "involves Payday lending that is utilizing the cloak of Indian Tribal sovereign immunity."

58. Corporate AML assigned an AML investigator, whose job responsibilities included the filing of SARs, to the matter. The investigator reported his findings in an email that was forwarded to the WBRM employee and multiple Corporate AML employees, including senior investigators. The investigator wrote that "it looks as though Mr. Tucker is quite the slippery individual" who "really does hide behind a bunch of shell companies." The investigator reported finding a former federal inmate named Scott A. Tucker who was "probably our guy" as well as "some old IRS liens for Mr. Tucker dating from 1991 and totaling about $150K" that were "released by 2001." The investigator noted that the Bank had "accounts for [Tucker's] wife" including a "personal Trust account (of course), a business account (SLK Services Inc) and an individual account." The investigator reported reading that Tucker "likes to put things in his wife's Trust's name (including some real estate)" and she "receives some periodic distributions from Black Creek Capital Corp [one of Tucker's wholly owned entities with an account at the Bank] in Henderson, NV which she moves to her Trust account and moves it on out from there."

59. The investigator also provided some information on Tucker's account activity. Regarding an account for one of Tucker's companies, the investigator noted that the money "comes in via large batches (list post totals) and goes out via checks and wires to mostly other apparently related accounts/businesses"—including one entity with a "very recently opened account and the only apparent purpose it apparently serves is to move money from" the account for Tucker's company to an account at another bank that the investigator hypothesized was

likewise controlled by Tucker. Finally, the investigator noted that Tucker is "fond of racing" and "sponsors (and drives for) a team called Level 5 Motorsports," which also had accounts at the Bank. The investigator noted that "one of his payday lending accounts wrote $940K worth of checks to Level 5 just since June. Every time he moves money out of [one of the Tribal Companies'] account[s] to another bank, he also writes a check to Level 5."

60. Based on these findings, the investigator concluded that Tucker "looks quite interesting" and was "probably a customer worth deeper investigation." The investigator stated that his first impression was that Tucker "could be less than honorable" and reiterated that he "controls quite a few large DDA accounts (holding tens of millions of dollars in each of them)" and "[j]udging from all the movement of money I found in just this preliminary glance he will be a difficult one to follow."

61. The Bank convened a working group to address the issues raised. After considering terminating its relationship with Tucker entirely, on October 11, 2011, the Bank decided to close the accounts in the names of the Tribal Companies—based on a concern for "reputational risk" to the Bank. The Tribal Companies' accounts, which accounted for the large majority of Treasury Management fees that USB received from the Tucker relationship, were closed on April 4, 2012, after Tucker found a new institution to house the subject accounts' funds. The Bank kept open Tucker's other accounts, including accounts for his other companies. USB also failed to file a SAR reflecting anything that it learned and conducted no historical review of the Tucker-controlled accounts' activity to determine whether it supported the assertions offered in the public news reports or its own investigator's initial review.

62. In April 2012, the Federal Trade Commission ("FTC") filed suit in U.S. District Court in the District of Nevada against Tucker, various Tribal Companies, and several other companies and individuals associated with Tucker. The lawsuit, which did not name the Bank as a party, alleged that the defendants violated federal law by, among other things, engaging in deceptive acts and practices in the marketing and offering of payday loans and deceptive collection practices in violation of the Federal Trade Commission Act, failing to properly disclose certain loan information in violation of the Truth in Lending Act and illegally conditioning the extension of credit on the preauthorization of recurring loans in violation of the Electronic Fund Transfer Act. The Bank failed to file a SAR after the FTC brought this action, which ultimately resulted in one of the Tribal Companies agreeing to pay $21 million and forgive customer debt, and the court granting summary judgment against Tucker and imposing a $1.26 billion judgment against him.

63. At these times, the Bank's policies provided that the Bank "must file a Suspicious Activity Report with FinCEN if the Bank 'knows, suspects or has reason to suspect' that a transaction, pattern o[f] transactions, or attempted transaction by, through, or to the financial institution involves: possible violations of a law or regulation; money laundering or BSA violations, including structuring transactions to avoid a BSA record keeping or reporting requirement; transactions that have no business or apparent lawful purpose that are unusual for the customer where there is no reasonable explanation; or the use of legal proceeds to facilitate criminal activity (e.g., terrorism)." The Bank's Bank Secrecy Act and Anti-Money Laundering Compliance Policy and Program in effect at the time (July 18, 2011) similarly recognized that all banks are required to file a SAR "when they know, suspect or have reason to suspect that there has been a transaction or attempted transaction involving money laundering, BSA violations, violations of law or regulations, the facilitation of criminal activity, or other suspicious activity."

64. After deciding to terminate its relationship with the Tribal Companies' accounts but retain Tucker as a client, the Bank opened numerous additional accounts for Tucker and his wholly-owned businesses. In opening these accounts, the Bank took no steps to ensure that money from the kind of activity that led the Bank to close the Tribal Companies' accounts would not continue to flow through the Bank. When opening the new accounts, the Bank failed to conduct meaningful due diligence. For example, in February 2013, the Bank opened accounts for two new Tucker-controlled entities. The only information USB received about the entities was that they were "Software Development" and "Management Services" companies owned and controlled by Tucker, as well as Articles of Incorporation listing, rather than Tucker, "Agent Services, Inc." as the Registered Agent and Managing Member.

65. In November 2013, the Office first served the Bank with a subpoena for Tucker- related accounts. Following receipt of this subpoena, the Bank engaged in an internal discussion concerning the remaining Tucker accounts and decided to discontinue the Bank's relationship with Tucker entirely.

66. On November 26, 2013, the Bank also filed its first SAR relating to Tucker- controlled accounts. In preparing the SAR, the Bank found that the sources of funding for the Tucker accounts still maintained by USB were "increasingly questionable income sources through payday loan businesses" that were "under investigation by the FTC." In only the year prior to this observation, the Bank found that the accounts had received "over $176,000,000.00 in domestic wire transfer, check or electronic deposits" and that a "large amount of funding to their accounts continues to be derived from their former payday loan businesses[.]"

67. The Government's investigation revealed that USB allowed Tucker to transfer approximately $230 million in proceeds of his criminal scheme into the Bank after deciding to close the accounts in the names of the Tribal Companies in October 2011.

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

IN THE MATTER OF:	)	
	)	
	)	
	)	**Number 2018-01**
U.S. Bank National Association	)	

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to assess a civil money penalty against U.S. Bank National Association (U.S. Bank or the Bank), pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to that Act.[1]

FinCEN has the authority to impose civil money penalties on financial institutions that violate the BSA. Rules implementing the BSA state that "[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" has been delegated by the Secretary of the Treasury to FinCEN.[2] At all times relevant to this Assessment, U.S. Bank was a "financial institution" and a "bank" within the meaning of the BSA and its implementing regulations.[3]

---

[1] The Bank Secrecy Act is codified at 12 U.S.C. §§ 1829b, 1951-1959 and 31 U.S.C. §§ 5311-5314, 5316-5332. Regulations implementing the Bank Secrecy Act appear at 31 C.F.R. Chapter X.

[2] 31 C.F.R. § 1010.810(a).

[3] 31 U.S.C. § 5312(a)(2)(A); 31 C.F.R. §§ 1010.100(d)(1), 1010.100(t)(1).

U.S. Bank is a full-service financial institution headquartered in Cincinnati, Ohio. As of September 30, 2017, the Bank had $452 billion in assets, over 70,000 employees, and 3,167 branches nationwide. U.S. Bank is the wholly owned subsidiary of U.S. Bancorp, a bank holding company based in Minneapolis, Minnesota, listed on the New York Stock Exchange under the ticker USB.

II. DETERMINATIONS

U.S. Bank willfully violated the BSA's program and reporting requirements from 2011 to 2015.[4] As described below, U.S. Bank failed to: (a) establish and implement an adequate anti-money laundering (AML) program from 2011 to 2014; (b) report suspicious activity from 2011 to 2014, and; (c) adequately report currency transactions from 2014 to 2015.

Rather than maintaining effective, risk-based policies, as required by the BSA, U.S. Bank devoted an inadequate amount of resources to its AML program from 2011 to 2014. First, the Bank capped the number of alerts its automated transaction monitoring system would generate for investigation. Testing indicated that these caps caused the Bank to fail to investigate and report large numbers of suspicious transactions. Nonetheless, instead of removing the alert caps, the Bank terminated the testing that demonstrated the caps' deficiencies. Similarly, from May 2009 until June 2014, U.S. Bank allowed non-customers to conduct currency transfers at its branches through a large money transmitter. Although the Bank knew that it had an obligation under the BSA to monitor those transfers for suspicious activity, it failed to include them in its

[4] 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. U.S. Bank is accused of "willfulness" herein only as the term is used in civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1).

automated transaction monitoring system. The Bank also employed inadequate procedures to identify and address high-risk customers that caused it to fail to effectively analyze and report the transactions of such customers.

The willfully deficient practices described above caused U.S. Bank to fail to file thousands of suspicious activity reports (SARs). A look-back analysis covering only a portion of the time-period during which these deficiencies persisted caused U.S. Bank to belatedly file more than 2,000 SARs on transactions worth more than $700 million. Some of these late-filed SARs identified transactions worth hundreds of thousands of dollars that potentially related to troubling criminal conduct.

Finally, from July 2014 until May 2015, U.S. Bank filed thousands of currency transaction reports (CTRs) that provided materially inaccurate information to FinCEN. Specifically, the CTRs failed to provide the names of the money services businesses (MSBs) that were the ultimate beneficiaries of the transactions. The Bank knew that the MSBs were the beneficiaries of the transactions, as it entered the MSBs' tax identification numbers (TINs) in the CTRs. Nevertheless, the Bank repeatedly entered the wrong beneficiary name in the CTRs, thus significantly undermining the utility of the CTRs for law enforcement purposes. The Bank allowed this problem to persist for nearly a year, resulting in thousands of materially inaccurate CTRs.

A. Violations of the Requirement to Develop and Implement an Anti-Money Laundering Program

U.S. Bank failed to establish and implement an adequate AML program as required by the BSA and its implementing regulations.[5] FinCEN requires banks to have an AML program

[5] 31 U.S.C §§ 5318(a)(2), 5318(h); 31 C.F.R. §1020.210.

that complies with the requirements imposed by its federal functional regulator. The Office of the Comptroller of the Currency (OCC), examines banks under its supervision for compliance with the Bank Secrecy Act under authority delegated from FinCEN. The OCC requires each bank to develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the BSA's recordkeeping and reporting requirements.[6] At a minimum, a bank's AML compliance program must: (a) provide for a system of internal controls to assure ongoing compliance; (b) provide for independent testing for compliance to be conducted by suitably independent bank personnel or by an outside party; (c) designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (d) provide for training of appropriate personnel.[7]

U.S. Bank failed to develop an AML compliance program that adequately covered at least two of the four pillars required by the BSA. The Bank had a deficient system of internal controls because, among other things, it failed to conduct risk-based monitoring of its customers' accounts and, instead, set fixed limits on the number of transactions that it would monitor for suspicious activity. *See infra* Part II.1.a. U.S. Bank also had inadequate staffing levels and outdated systems to conduct appropriate monitoring and due diligence, manage alerts for suspicious activity, and handle law enforcement inquiries. *See infra* Part II.2. Finally, U.S. Bank, among other things, failed to have its automated transaction monitoring system validated by a suitably independent individual (or entity), notwithstanding an express regulatory recommendation. *See infra* Part II.3.

---

[6] 12 C.F.R. § 21.21.

[7] Id.

1. Internal Controls

a. Transaction monitoring for suspicious activity

U.S. Bank failed to conduct risk-based transaction monitoring and, as a result, did not identify significant amounts of suspicious activity that it should have uncovered. Since April 2004, USB used Searchspace, a commercially available software system for monitoring transactions flowing through the Bank. From at least 2009 until July 2014, U.S. Bank configured this automated transaction monitoring system to generate a certain number of alerts each month. In addition, out of the 22 scenario-based queries U.S. Bank set-up for alert generation, the Bank set caps on the six largest alert generators and retained those caps even when below-threshold testing[8] demonstrated significant missed SAR reporting.

As a result of the alert limits, the transaction monitoring systems did not generate alerts for many of the transactions that an appropriate risk-based approach would have flagged as potentially suspicious. Ultimately, the Bank's suppression of a substantial number of alerts prevented the Bank from investigating and reporting suspicious activity. Nonetheless, the Bank failed to address the numerical caps because those fixed caps permitted the Bank to hire fewer employees and investigators in its AML department.

The Bank's alert suppression described above caused it to fail to investigate large amounts of potentially suspicious activity. A 90-day rule the Bank implemented as a re-alerting policy caused the system to prevent the generation of new alerts. Queries[9] on accounts that had

[8] At U.S. Bank, below-threshold testing involved selecting a sampling of alerts occurring immediately below the alert thresholds – alerts that were not ordinarily being investigated given the thresholds that were in place – and then having investigators review them in order to determine whether the thresholds should be lowered because they were causing a substantial amount of suspicious activity to be missed.

[9] At U.S. Bank, Queries were "rules" that were run against transaction data in its monitoring software (Searchspace) to identify indicia of potentially suspicious activity.

generated an alert within the last 90 days did not generate a new alert, regardless of how suspicious the activity appeared to be or whether the prior alert resulted in a SAR. A limited review focused on three sample queries in 2013 concluded that the Bank's 90-day rule suppressed approximately 6,888 "productive" alerts. Moreover, U.S. Bank failed to review a significant number of the alerts its system generated. A review conducted on wire transfer activity in June 2013 found that, of the over 57,000 customers (some of which may be duplicates) that alerted, the Bank reviewed less than 100 for suspicious activity determination. Finally, the look-back review the Bank conducted, which focused largely on six-month periods from 2013 to 2014, concluded that alert suppression prevented the Bank from reporting over $318 million in suspicious activity. This suspicious activity resulted in late filing of 1,528 SARs.

Moreover, the Bank knew that its alert suppressions were causing it to fail to investigate — and file SARs on — a significant number of suspicious transactions. From 2007 through April 2012, U.S. Bank conducted "below-threshold" testing to evaluate the extent to which the limits placed on alerts for Queries caused the Bank to fail to investigate and file SARs on suspicious activity. The below-threshold test involved selecting a sample of alerts that occurred immediately below the alert limits to determine whether the limits should be adjusted to capture suspicious activity that occurred below the threshold. This below-threshold testing found a significant amount of suspicious activity occurring below the alert limits that the Bank employed. For example, in November 2011, the Bank's AML staff concluded that, during the past year, an average of 50% of the transactions that were reviewed during the below-threshold testing resulted in the filing of a SAR.

Based on the results of the below-threshold testing, certain Bank employees wanted to lower the alert thresholds to increase the number of alerts reviewed and ensure that the Bank

properly investigated and reported suspicious activity. Nonetheless, the Bank failed to properly address the concerns raised by below-threshold testing. In fact, rather than reducing alert thresholds and investigating a larger number of transactions, the Bank decided to stop conducting below threshold testing in April 2012. The Bank's internal explanation for that decision ignored previous management communications regarding the likelihood of regulatory scrutiny of its fixed numerical caps. For example, as the Bank's AML Officer (AMLO) wrote to its Chief Compliance Officer (CCO) on December 1, 2009, a "regulator could very easily argue that [below-threshold] testing should lead to an increase in the number of queries worked." The Bank terminated its below-threshold testing because that testing showed that the Bank was failing to address an ongoing problem.

U.S. Bank maintained its alert caps because the practice permitted the Bank to devote fewer employees and resources to its AML program. For example, internal notes of an AML employee state: "The number of query alerts that we work are increasingly [sic] based solely on staffing levels. This is a risk item." For much of the relevant period, U.S. Bank had between 25 to 30 AML investigators. Apart from those investigators added as a result of acquiring other banks, U.S. Bank did not substantially increase its number of investigators. As late as 2012, when U.S. Bank had over $340 billion in assets, the Bank had only 30 investigators. U.S. Bank also failed to increase salaries of certain AML employees even after human resources and compliance personnel complained to the CCO that the Bank was paying its investigators below-market salaries and competitor banks were successfully poaching U.S. Bank investigators. The CCO and AMLO understood that the Bank's failure to hire additional staff created significant AML risks. For example, the December 2009 memo from the AMLO to the CCO acknowledged that, even though the Bank had seen significant increases in SAR volume, law enforcement

inquiries, and closure recommendations, "staffing levels have remained relatively constant." According to the AMLO, the combination of these factors resulted in an "increased workload" for "staff that already is stretched dangerously thin." The AMLO also explicitly referenced alert caps, describing the trends discussed above as "especially distressing give[n] the fact that an increase in the number of alerts worked is imminent and necessary." Nonetheless, as described above, U.S. Bank neither removed alert caps nor hired an adequate number of AML employees for several years after December 2009.

The U.S. Bank CCO and AMLO recognized that the alert caps, in addition to causing the Bank to fail to investigate and report large amounts of potentially suspicious activity, also was at odds with the expectations of regulators. The OCC warned U.S. Bank on several occasions that managing the Bank's monitoring programs to the size of its staff and other resources would get the Bank in trouble with the OCC. To avoid regulatory problems, U.S. Bank took steps to avoid disclosing the alert caps to the OCC. In 2012, when the Bank hired new officials to oversee its AML program, their predecessors, including the CCO, discouraged them from removing the alert caps or disclosing them by representing to the new officials that its regulators were fully aware of the Bank's monitoring practices and had at least tacitly approved them. More broadly, driven in large measure by instructions from the CCO, compliance employees consistently did not volunteer information to regulators, including deficiencies with transaction monitoring, except in response to specific requests. In 2013 memo, the AMLO described U.S. Bank's AML program as an effort to use "smoke and mirrors" to "pull the wool over the eyes" of the OCC.

In 2013, Bank employees prepared a PowerPoint presentation for the CEO that identified multiple vulnerabilities in the Bank's AML program, and explained how those same problems led to actions against other banks. The PowerPoint presentation explicitly referred to, among

other things, "[m]anipulation of system output through use of alert caps on both profiling and query detection methods" that could "potentially result in missed Suspicious Activity Reports" and "[p]otential regulatory action resulting in fines, consent order, and significant historical review of transactions." However, the CCO reviewed a draft and removed references to alert caps from the presentation, added positive information about the Bank's AML program, and otherwise altered the presentation to depict a more favorable image of the Bank's AML program.

In addition to maintaining inappropriate alert caps, U.S. Bank also failed to monitor transactions conducted at its branches through a large money transmitter. From May 2009 until July 2014, U.S. Bank allowed both customers and non-customers to conduct currency transfers at U.S. Bank branches through the money transmitter. Based on an internal memo, the Bank recognized that such currency transfers were one of the riskiest products offered by the Bank, and that, to the extent such transfers were conducted by non-customers, they would not be processed through the Bank's automated transaction monitoring system. The Bank nonetheless continued to process currency transfers for non-customers without adequate controls to mitigate risks until July 2014. Moreover, even though Bank employees had referred these currency transfers to compliance for a suspicious activity reporting review, these referrals were not investigated by the Bank's AML department until June 2013.

Notably, in December 2012, the new AMLO emailed the CCO with concerns about monitoring in connection with the above-referenced money transmitter. In response, the CCO dismissed the new AMLO's concerns and chastised him for recording them in an email.

The look-back analysis that the Bank conducted showed that, for the six-month period analyzed, U.S. Bank's failure to monitor currency transfers at its facilities for transactions involving the large money transmitter caused it not to detect and report over $12 million in

suspicious transactions. For the reasons described above, U.S. Bank violated the BSA's requirement to properly detect and report suspicious activity.

b. Customer due diligence program

U.S. Bank also had inadequate processes and procedures to identify and address high-risk customers. The Bank's customer risk-rating program failed to review customer relationships in their entirety — i.e., across the Bank's different business lines — in order to obtain an enterprise-wide view of customer risk. In addition, the Bank failed to include important information about its clients in its risk-rating analysis, such as a customer's country of citizenship and occupation. The exclusion of this information resulted in high-risk customers being risk-rated based on incomplete information. As a result, customers whom the Bank identified or should have identified as high-risk were free to conduct transactions through the Bank with insufficient oversight.

As part of a look-back analysis, the Bank analyzed transactions involving high-risk customers that it had previously failed to identify and investigate properly. Though the transactions covered a limited time-period (from May 2014 through April 2015), it resulted in the Bank late filing more than 136 SARs on transactions/customers that the Bank previously overlooked.

2. Designation of individuals responsible for day-to-day BSA compliance

From 2007 through 2014, due in part to the actions of its CCO, U.S. Bank failed to designate sufficient resources, in terms of staff levels, budget, and systems commensurate with the Bank's AML risks inherent in its size, complexity, products and services. A bank is required to designate individual or individuals responsible for ensuring day-to-day compliance with BSA

requirements.[10] The requirement extends beyond the actual designation of a person to fulfill this role. Appointing a BSA officer is not sufficient to meet the regulatory requirement if that person does not have sufficient authority, resources, or time to satisfactorily complete the job.

U.S. Bank had inadequate staffing levels to manage alerts for suspicious activity and handle law enforcement inquiries. U.S. Bank had approximately 30 investigators and often times struggled to retain its limited BSA staff. U.S. Bank's CCO and AMLO were fully aware of the situation, as compliance and human resources employees raised related concerns for several years but the Bank ignored those concerns. Further, a 2009 memo submitted by the AMLO to the CCO regarding increased workload in the BSA Department, raised concerns that the significant increase in alerts had not coincided with an increase in AML staffing levels. In the memo, the AMLO projected alerts to increase by 47%, law enforcement inquiries to increase by 123%, and closure recommendations to be 160% higher. The AMLO further stated these alerts projections would result in an increased workload that is not proportionate with the staff levels at the Bank. In April 2010, the AMLO again reached out to the CCO with a memo concerning the increased AML workload. In the same memo, the AMLO requested the opportunity to speak with the CCO about adding additional staff to meet the increased workload. Instead of providing the needed resources, the CCO chose to tailor its monitoring process and alert reviews to fit the capability of its understaffed BSA Department. As a result, the Bank suppressed an alarming number of alerts and failed to investigate and report potentially suspicious activity.

During that time, U.S. Bank had AML leadership that failed to actively support compliance efforts, manage and mitigate BSA deficiencies, and ensure that risk mitigation were not compromised by revenue interests.

---

[10] 31 U.S.C. § 5318(h)(1)(B); 31 C.F.R. § 1020.210.

3. Independent Validation

U.S. Bank also failed to provide for independent validation of its automated transaction monitoring system. Specifically, despite recommendations from the OCC dating back to 2008, the Bank failed to have SearchSpace independently validated. For example, in connection with an OCC review of SearchSpace in 2008, the OCC found that "Management has not validated SearchSpace in accordance with OCC Bulletin 2000-16 Model Validation." The OCC discussed the results of this review with, among others, the CCO and AMLO. Thereafter, in connection with another review of SearchSpace in 2010, the OCC concluded that although "Management [had] validated Searchspace" since the OCC's 2008 review, "the individual who completed the validation [was not] independent, given his primary responsibilities surrounding the Searchspace system." The OCC recommended that the Bank complete an independent validation of SearchSpace, and it again discussed the results of its review with, among others, the CCO and AMLO. The Bank, however, did not have Searchspace independently validated at that time.

Not only did the Bank fail to follow the OCC's recommendation that it conduct independent validation, but it had one of its employees conduct "validations" of SearchSpace that were plainly insufficient. After the OCC's 2010 review, and continuing into 2013, the Bank employee who was responsible for managing SearchSpace (the "SpearchSpace Manager") prepared a "biannual SearchSpace Model validation" and asked another Bank employee (the "Other Employee") to review it and acknowledge having done so, while assuring the Other Employee that he was "not making any representation that [he was] validating anything." For purposes of these biannual reviews, the Other Employee merely "read [the SearchSpace Manager's] documentation and sign[ed] off that . . . they ma[d]e sense and that [he] believe[d] they [were] accurate."

While U.S. Bank was engaging in this deficient validation process, the SearchSpace Manager stated to the Other Employee that a regulator "could (and probably will at some point), force us to hire outside auditors to perform a more robust independent validation/review," but "this would cost tens of thousands . . . minimum." The SearchSpace Manager told the Other Employee that "[u]ntil we are forced to go there . . . you are sufficient."

B. Violation of the Requirement to File Currency Transaction Reports

U.S. Bank violated its currency transaction reporting requirements. The BSA and its implementing regulations impose an obligation on financial institutions to report currency transactions that involve or aggregate to more than $10,000 in one business day.[11] A bank must file a CTR within 15 days after the transaction triggering the reporting requirement is conducted.[12] Reports required by section 1010.311 shall be filed on forms prescribed by the Secretary of the Treasury and "all information called for in such forms shall be furnished."[13]

From July 7, 2014 through May 27, 2015, U.S. Bank filed approximately 5,000 CTRs with incomplete and inaccurate information. CTR reporting requirements play a major role in FinCEN's core mission to safeguard the financial system from illicit use through the collection, analysis, and dissemination of financial intelligence. As cash-intensive businesses are criminal organizations' method of choice in an attempt to legitimize illegal cash transactions, FinCEN and law enforcement depend on the accurate and timely filing of CTRs by financial institutions to establish and follow a trail documenting the movement of illicit funds. FinCEN also relies on CTRs to monitor the compliance of regulated financial institutions and to identify potential areas

[11] 31 U.S.C. § 5313(a); 31 C.F.R. §§ 1010.311, 1010.313.

[12] 31 C.F.R. § 1020.310; 31 C.F.R. § 1010.306(a)(1).

[13] 31 C.F.R. § 1010.306(d).

of BSA/AML risk in the U.S. financial system. Specifically, in filling out CTRs, the Bank failed to accurately identify the name of the entity on whose behalf the transaction was conducted. The Bank continued to list the name of its domestic respondent bank as the person on whose behalf the funds were deposited despite knowing that the funds were ultimately those of non-customers of U.S. Bank. In most cases, the non-customers were credit unions, and, for at least $600 million of the currency transactions, the entities on whose behalf the transactions were being conducted were MSBs. The Bank knew that the ultimate beneficiaries of the transactions were MSBs but the Bank misidentified the name of the entity despite including an accurate taxpayer identification number. The Bank wrongly reported those TINs as belonging to the respondent bank. By filing the CTRs in this manner, U.S. Bank impeded law enforcement's and FinCEN's ability to identify and track potentially unlawful behavior, as a search of the CTRs using the names of the relevant MSBs would have yielded no responses. The transactions underlying these CTRs involved more than $600 million and demonstrated a systemic failure to comply with BSA reporting requirements.

C. Violations of the Requirement to Report Suspicious Transactions

The BSA requires banks to report transactions that involve or aggregate to at least $5,000, that are conducted "by, at, or through" the bank, and that the bank "knows, suspects, or has reason to suspect" are suspicious.[14] A transaction is "suspicious" if the transaction: (a) involves funds derived from illegal activities, or is conducted to disguise funds derived from illegal activities; (b) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations under the Act; or (c) has no business or apparent lawful purpose or is not the

[14] 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320.

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 the background and possible purpose of the transaction.[15]

As described above, U.S. Bank had defects in its customer risk-rating program, imposed inappropriate caps on the number of transaction alerts it would investigate, and failed to review funds transmission that non-customers conducted at U.S. Bank facilities through a large money transmitter. These willfully deficient monitoring practices caused the Bank to fail to file over 2,000 SARs on transactions worth hundreds of millions of dollars. U.S. Bank also failed to report on suspicious activity of customers using its cash vault services on transactions related to suspected narcotics activity, and wire transfers from high-risk jurisdictions in Latin America and Africa.

U.S. Bank conducted several look-back analyses relating to its deficient monitoring practices. Through these look-backs, the Bank examined historical transactions to determine the extent to which transaction monitoring defects identified herein caused it to fail to file SARs on suspicious transactions. Each look-back analysis examined a six-month period, and thus covered only a portion of the time period during which the deficient monitoring practices persisted. In total, the look-back analyses examined (i) 1.7 billion demand deposit account transactions, (ii) 650,000 transactions conducted through the above-referenced large money transmitter, and (iii) 250,000 "cash vault" transactions that included current and historical high-risk customers. The look-back analyses resulted in the creation of more than 24,000 alerts on transactions that the Bank had previously failed to review.

[15] 31 C.F.R. § 1020.320(a)(2)(i) – (iii).

Based on the findings of its look-back analyses, U.S. Bank late filed a total of 2,121 SARs reporting more than $700 million in suspicious activity. Some of these late SAR filings described a variety of illicit activities involved in transactions conducted by U.S. Bank's customers. The following bullets provide further detail on the Bank's look-back analyses and its corresponding late filing of the 2,121 SARs:

- **High Risk Customers and Cash Vault Services.** The Bank's look-back analysis concerning high-risk customers covered two periods between May 2014 and April 2015. As a result of these look-backs, the Bank late filed 162 SARs on transactions of more than $380 million.
- **Alert Caps.** The Bank's look-back analysis relating to alert caps in its automated monitoring software covered several different six-month periods falling between July 2012 and June 2014. This look-back required the Bank to late file 987 SARs on transaction worth over $220 million. Separately, the Bank performed a look-back analysis relating to queries that covered the period from September 2015 through February 2016. Consequently, the Bank late file 541 additional SARs on transactions involving more than $90 million.
- **The Large Money Transmitter.** The Bank's look-back analysis concerning the large money transmitter covered the period between January and June 2014. That analysis caused the Bank to late file 431 SARs on transactions involving more than $12 million.

As noted above, these look-back analyses covered only six-month periods. A further analysis of the remainder of the period during which U.S. Bank maintained each willfully deficient monitoring practice would have identified many more instances in which it had failed

to file SARs. Indeed, in or about 2014, a third-party consultant retained by the Bank sampled 68 accounts that Queries had flagged in 2013 but had not alerted because the accounts fell below the alert limits, and found that 26 of the accounts (38%) were "productive or potentially productive," meaning that, for those accounts, the consultant was unable to identify a reasonable explanation for the unusual alert activity. The third-party consultant also tested a sample of Internal Referral Forms (IRFs) that Bank employees had completed for non-customer money transfers using the above-referenced large money transmitter, and the consultant concluded that, by failing to review such IRFs, the Bank had failed to file approximately 77 SARs during the June 2009 through December 2011 time-period.

Notably, the additional SARs that U.S. Bank filed as a result of its look-back analyses reported troubling potential criminal activity. These instances of potential criminal activity demonstrate that SARs, like other BSA filings, play an important role in law enforcement and regulatory matters. FinCEN and law enforcement use SARs to investigate money laundering, terrorist financing, and other serious criminal activity.

III. RESOLUTION WITH THE OFFICE OF THE COMPTROLLER OF THE CURRENCY AND THE DEPARTMENT OF JUSTICE

The OCC is U.S. Bank's federal functional regulator and is responsible for conducting examinations of U.S. Bank for compliance with the BSA and its implementing regulations and similar rules under Title 12 of the United States Code. In October 2015, the Bank entered into a consent order with the OCC based on various deficiencies in its AML compliance program, including gaps in suspicious activity monitoring, insufficient staffing and inadequate monitoring of transactions through the large money transmitter. On February 15, 2018, the OCC assessed a $75 million civil money penalty against U.S. Bank in connection with those violations.

On February 15, 2018, U.S. Bancorp, US Bank's parent corporation, entered into a Deferred Prosecution Agreement ("DPA") with the Criminal Division of the United States Attorney's Office for the Southern District of New York based on charges that, beginning no later than 2009 and continuing until 2014, it, through the Bank, willfully failed to implement an effective AML program, in violation of 31 U.S.C. § 5318(h), and failed to file SARs, in violation of 31 U.S.C. § 5318(g). As part of the DPA, U.S. Bancorp agreed to forfeit $528 million and admitted that it, through the Bank, had "willfully (i) failed to maintain an effective [AML] program and (ii) failed to report suspicious transactions relevant to a possible law or regulations as required by the Secretary of the Treasury."

IV. CIVIL MONEY PENALTY

FinCEN has determined that U.S. Bank willfully violated the program and reporting requirements of the BSA and its implementing regulations as described in this ASSESSMENT, and that grounds exist to assess a civil money penalty for these violations.[16]

FinCEN considered the size and sophistication of U.S. Bank, one of the largest depository institutions in the United States. Furthermore, FinCEN noted the severity and duration of U.S. Bank's BSA violations. For several years, the Bank continued to implement an inadequate BSA/AML program, with deficiencies in internal controls. In addition, FinCEN had previously communicated to the industry that the practice of artificially limiting compliance staff, including by setting staff-based numerical caps for alerts, was considered reckless.

FinCEN considered U.S. Bank's continued cooperation with FinCEN, the OCC, and the U.S. Attorney's Office for the Southern District of New York during the course of its

[16] 31 U.S.C. § 5321; 31 C.F.R. § 1010.820.

investigation. FinCEN also recognized that the Bank made significant investments in BSA/AML staffing and technology and has contributed significantly to other high-priority law enforcement and FinCEN actions for which it has received notable recognition. U.S. Bank has demonstrated a commitment and ability to correct the issues found in this Assessment with its implementation of significant remedial efforts.

In December 2017, FinCEN and U.S. Bank entered into a tolling agreement, pursuant to which the parties agreed that any statute of limitations applicable to the claims at issue here would be tolled from and including December 7, 2017, through and including June 7, 2018. Accordingly, FinCEN is entitled to base its penalty assessment against U.S. Bank on conduct occurring from and including December 7, 2011, through and including the date of this Assessment.[17]

FinCEN has determined that the penalty in this matter will be $185 million. U.S. Bank's obligation to pay that amount will be deemed satisfied if, within thirty (30) business days of the Effective Date, (a) it pays $70 million (seventy million dollars) to the Treasury Department and (b) U.S. Bancorp pays the United States the full amount it is required to pay under the DPA, pursuant to the terms of the DPA.

V. CONSENT TO ASSESSMENT

To resolve this matter, U.S. Bank has entered into a Stipulation and Order of Settlement and Dismissal with the Civil Division of the United States Attorney's Office for the Southern District of New York ("Settlement Agreement").

[17] 31 U.S.C. § 5321(b).

VI. PUBLIC STATEMENTS

U.S. Bank, having truthfully admitted to the facts set forth in Paragraphs 2 & 3 of the Settlement Agreement ("Admissions"), agrees that it shall not take any action or make any public statements contradicting or denying, directly or indirectly, the Admissions. Any material failure to comply with this requirement shall entitle FinCEN to pursue the remedies set forth in Paragraph 10 of the Settlement Agreement.

VII. RELEASE

Upon final execution of the Settlement Agreement by the United States District Court for the Southern District of New York, FinCEN releases U.S. Bank from any civil or administrative claim for monetary or injunctive relief under the BSA as set forth in Paragraphs 8 & 9 of the Settlement Agreement.

/s/ 2/15/18

Kenneth A. Blanco Date
Director
Financial Crimes Enforcement Network (FinCEN)
U.S. Department of the Treasury

Steptoe

INTERNATIONAL LAW ADVISORY

FinCEN Penalizes Compliance Officer for Anti-Money Laundering Failures

March 24, 2020

Authors

Zoe Osborne, Jack R. Hayes, Nicholas Turner

Overview

On March 4, the Financial Crimes Enforcement Network (FinCEN) of the US Treasury Department imposed a $450,000 civil money penalty against Michael LaFontaine, former chief operational risk officer at US Bank National Association (US Bank), for his alleged role in failing to prevent violations of US anti-money laundering (AML) laws and regulations that occurred during his tenure. FinCEN's unprecedented individual enforcement action is the latest sign that US AML regulators intend to hold individual executives accountable for their roles in financial institutions' violations of law. It serves as a reminder of the importance of strengthening compliance programs in order to minimize the likelihood of findings of individual liability.

The threat is especially real for individuals in large financial institutions, even though executive and other high-level officers are less likely to be involved in daily decision-making at issue in institution-wide enforcement actions. For example, in a 2017 press statement announcing its settlement of AML violations with former MoneyGram chief compliance officer, the then-acting director of FinCEN noted that:

> "We have repeatedly said that when we take an action against an individual, the record will clearly reflect the basis for that action. Here, despite being presented with various ways to address clearly illicit use of the financial institution, the individual failed to take required actions designed to guard the very system he was charged with protecting, undermining the purposes of the BSA. Holding him personally accountable strengthens the compliance profession by demonstrating that behavior like this is not tolerated within the ranks of compliance professionals."

As detailed in FinCEN's Assessment of Civil Money Penalty (the Assessment), the action against LaFontaine follows a deferred prosecution agreement between US Bancorp – the parent company of US Bank – and the US Department of Justice over related criminal charges in 2018 (for more analysis on that enforcement action, see Steptoe's March 2018 Client Advisory).

The Civil Money Penalty

LaFontaine held senior positions in US Bank's AML department from 2005 until his separation from the bank in 2014. According to FinCEN, LaFontaine's roles involved progressively more responsibility over time and included positions as chief compliance officer (CCO), followed by senior vice president and deputy risk officer, and finally executive vice president and chief operational risk officer. As the chief operational risk officer, LaFontaine reported directly to US Bank's CEO and had direct communications with its board of directors. LaFontaine also had primary responsibility for overseeing US Bank's AML compliance department, and for supervising the Bank's CCO, AML officer (AMLO), and AML staff.

Due to his oversight responsibility, FinCEN determined that LaFontaine purportedly shared responsibility for US Bank's violations, including failures to maintain an effective AML program and to properly file Suspicious Activity Reports (SARs) as required by the US Bank Secrecy Act (BSA) and FinCEN's implementing regulations. This included failures to:

- Implement and maintain an adequate AML program
- Adequately staff the program with AML compliance investigators
- Timely file thousands of SARS

Notably, the Assessment states LaFontaine admitted that the bank violated the BSA, that he participated in these violations, and that the conduct demonstrated recklessness or disregard.

Failure to Ensure Sufficient AML Resources

FinCEN alleges that US Bank failed to implement and maintain an adequate AML program by, *inter alia*, maintaining policies, procedures, and controls that the bank knew would result in its failure to investigate and report suspicious and potentially illegal activity involving customer accounts. Alleged activity included: (a) imposing upper limits on the number of alerts produced by the institution's automated transaction monitoring system; (b) not subjecting Western Union money transfers to the monitoring system; and (c) inadequately identifying and monitoring high-risk customers in compliance with the BSA.

In addition to these program deficiencies, FinCEN alleges that US Bank "employed a woefully inadequate number of AML investigators." FinCEN suggests that "Mr. LaFontaine was put on notice of this situation through internal memos from staff claiming that significant increases in SAR volumes, law enforcement inquiries, and closure recommendations created a situation where AML staff was 'stretched dangerously thin.'" According to the Assessment, LaFontaine failed to act "when presented with significant AML program deficiencies in . . . the number of staff to fulfill the AML compliance role."

LaFontaine's Role in SARs Failures

US Bank's AML department used SearchSpace, a commercially available software system, to monitor transactions flowing through the bank for indicators of potential money laundering and other types of illicit conduct. In order to justify hiring fewer AML employees and investigators, US Bank's management decided to institute a cap on the number of alerts generated by the system. As a result of this cap, the SearchSpace software did not generate alerts on many accounts or high-risk customers that FinCEN alleges should have been reviewed or flagged as potentially suspicious.

In the Assessment, FinCEN states that US Bank knew its alert limits were causing a failure to investigate and file SARs on a significant number of potentially suspicious transactions. Moreover, from 2007 through April 2012, US Bank staff conducted "below-threshold testing" to evaluate the extent to which the caps were suppressing alerts on potentially suspicious transactions and found that "a significant amount of suspicious activity occurring below the alert limits that the Bank had employed."

Further, FinCEN alleges that "LaFontaine was warned by his subordinates and by regulators that capping the number of alerts was dangerous and ill-advised." *See* FinCEN Press Release. The Assessment notes that the Office of the Comptroller of the Currency (OCC) of the US Treasury Department had repeatedly warned US Bank that "using numerical caps to limit the Bank's monitoring programs based on the size of its staff and available resources could result in a potential enforcement action and FinCEN had taken previous public actions against banks for the same activity."

Despite these warnings, US Bank allegedly did not begin to address its deficient policies and procedures until June 2014, when questions from the OCC and reports from an internal whistleblower caused US Bank to retain outside counsel. According to FinCEN Director Kenneth A. Blanco, as quoted in the FinCEN Press Release, these actions "prevented the proper filing of many, many SARs, which hindered law enforcement's ability to fully combat crimes and protect people . . . ."

Compliance Takeaways

Below are our key takeaways from FinCEN's enforcement action:

1. Ensure the Compliance Unit is Appropriately Staffed to Meet BSA Requirements

Despite having more than $340 billion in assets, US Bank employed approximately 30 AML investigators at the time of the violations. FinCEN described this as a "woefully inadequate number," which contributed to the bank's alleged violations of the BSA's requirement to provide the compliance officer with sufficient resources to fulfill his or her responsibilities. Additionally, inadequate staffing can leave potentially suspicious activity undetected, increasing the possibility of violating the BSA and FinCEN's requirements to file timely SARs.

2. Ensure Technology is Appropriately Calibrated to Flag Suspicious Activity

According to Director Blanco, as quoted in the FinCEN press release, "FinCEN encourages technological innovations to help fight money laundering, but technology must be used properly." US financial institutions should test the accuracy of any software used to identify potentially suspicious activity to ensure that it is properly calibrated. This applies to both AML and sanctions technology.

3. Escalate Internal Warnings

3. Escalate Internal Warnings

In its Assessment, FinCEN highlighted the fact that LaFontaine was made aware by numerous employees — including the CCO and AMLO — and even US regulators that US Bank's cap on transaction monitoring alerts presented a serious risk. The CCO and AMLO also informed LaFontaine that US Bank should be acting as though it were "under a virtual OCC consent order." As demonstrated by this case, FinCEN will hold compliance officers (and not just their employers) responsible for violations of the BSA. Companies of all stripes can learn from US Bank's experience by creating proper internal channels for staff to escalate and remedy potential AML program deficiencies.

4. Take Heed from Other Enforcement Actions

FinCEN notes in the Assessment that FinCEN brought action against Wachovia Bank for similar conduct during the same period US Bank's violations were occurring. Like US Bank, Wachovia had improperly capped the number of alerts generated by its automated transaction monitoring system, "fail[ing] to adequately staff the BSA compliance function," and employed "as few as three individuals' to monitor all of Wachovia's 'correspondent relationship with foreign national institutions.'" FinCEN therefore concluded that LaFontaine "should have known based on his position the relevance of the Wachovia action to US Bank's practices or conducted further diligence to make an appropriate determination." FinCEN's conclusion makes clear its expectation that US financial institutions, and particularly compliance officers responsible for supervising an adequate AML program, stay abreast of enforcement actions and use this information to identify and correct their own potential violations.

It is not only authorities in the United States that are placing an increased focus on AML failings and the individuals potentially liable for those failings. In Europe and the UK, for example, the Fifth Money Laundering Directive (5MLD) took effect on January 10, 2020. The 5MLD proposals require, among other things, that EU members states (which includes the UK for these purposes) introduce a newly defined set of enhanced due diligence measures, to identify beneficial owners of companies and to maintain public registers of these, and to record the identities of virtual currency owners. Enforcement actions against individuals are also expected to rise. In the UK, for example, the director of the Financial Conduct Authority has expressed the agency's desire to give "effect to the full intention of the Money-Laundering Regulations which provides for criminal prosecutions." The Financial Conduct Authority has the power to criminally prosecute a person or organization it suspects of not putting in place sufficient safeguards against money laundering. Anyone found guilty is liable to receive a fine and up to two years' imprisonment.

For additional information on these issues, including ensuring an adequate compliance program, follow the Steptoe International Regulation and Compliance (IRC) Blog or contact one of our lawyers located in the United States, Europe (London and Brussels), and Asia (Beijing and Hong Kong).

Practices

Anti-Money Laundering

Independent & Internal Investigations

FCPA/Anti-Corruption

Financial Services