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. <u>Violation of the Requirement to File Currency Transaction Reports</u>

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. <u>Violations of the Requirement to Report Suspicious Transactions</u>

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