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

IN THE MATTER OF:	)	
	)	
	)	
	)	**Number 2017-02**
Merchants Bank of California, N.A.	)	
Carson, California	)	

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 Merchants Bank of California, N.A. (Merchants or the Bank), pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to that Act.[1]

Merchants admits to the facts set forth below and that its conduct violated the BSA.[2] Merchants consents to this assessment of a civil money penalty and entered into the CONSENT TO THE ASSESSMENT OF CIVIL MONEY PENALTY (CONSENT) with FinCEN.

The CONSENT is incorporated into this ASSESSMENT OF CIVIL MONEY PENALTY (ASSESSMENT) by reference.

FinCEN has the authority to investigate banks for compliance with and violation of the BSA pursuant to 31 C.F.R. § 1010.810, which grants FinCEN "[o]verall authority for

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

[2] Merchants makes the admissions as stated above and elsewhere in this document solely in connection with the resolution of this civil proceeding and for purposes of the imposition of the civil money penalty set forth herein.

enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter. . . ."

Merchants is a "financial institution" and a "bank" within the meaning of the BSA and its implementing regulations during the time relevant to this action.[3]

Merchants is a community bank located in Carson, California, that provides business, personal, and electronic banking services. As of September 30, 2016, Merchants had over $64 million in total assets and one location with 46 employees.

Resolution with the Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency (OCC) is Merchants's Federal functional regulator and is responsible for conducting examinations of Merchants for compliance with the BSA and its implementing regulations and similar rules under Title 12 of the United States Code. The OCC has identified deficiencies in the Bank's practices that resulted in violations of the consent orders entered into by the Bank on June 23, 2010, and June 26, 2014, as well as a continued violation of 12 C.F.R. § 21.21. The OCC is simultaneously assessing a civil money penalty against Merchants for these violations.

II. DETERMINATIONS

Merchants willfully violated the BSA's program and reporting requirements from March 2012 to September 2016.[4] As described below, Merchants failed to (a) establish and implement an adequate AML program; (b) conduct required due diligence on its foreign correspondent

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

[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. Merchants admits to "willfulness" only as the term is used in civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1).

accounts; and (c) detect and report suspicious activity. Merchants's failures allowed billions of dollars in transactions to flow through the U.S. financial system without effective monitoring to adequately detect and report suspicious activity. Many of these transactions were conducted on behalf of money services businesses (MSBs) that were owned or managed by Bank insiders who encouraged staff to process these transactions without question or face potential dismissal or retaliation.

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

Merchants failed to establish and implement an adequate AML program as required by the BSA and its implementing regulations.[5] The OCC requires each bank under its supervision 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 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 training for appropriate personnel.[7]

Merchants failed to establish and maintain adequate internal controls to assure ongoing compliance. The Bank did not conduct a sufficient independent audit commensurate with the

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

[6] 12 C.F.R. § 21.21.

[7] 31 U.S.C. §§ 5318(a)(2), 5318(h)(1); 31 C.F.R. § 1020.210; 12 C.F.R. § 21.21.

Bank's complexity and risk profile; it failed to provide the necessary level of authority, independence and responsibility to its BSA Officer to ensure day-to-day compliance; and it did not provide adequate training for appropriate personnel.[8]

1. Internal Controls

Merchants failed to implement an effective system of internal controls reasonably designed to ensure compliance with the BSA.[9] Merchants provided banking services for as many as 165 check-cashing customers and 44 money transmitters, many of which were located hundreds of miles away from Merchants. The Bank did so without adequately assessing the money laundering risk of these customers and designing an effective AML program to address those risks. Specifically, it did not implement adequate due diligence programs and provided its high-risk customers with remote deposit capture services (RDC) without adequate procedures for monitoring their use.

In several instances, Bank insiders directly interfered with the BSA staff's attempts to investigate suspicious activity related to insider-owned accounts. Bank insiders owned or managed MSBs, which had accounts at Merchants. From 2007 to September 2016 certain of these accounts demonstrated highly suspicious transaction patterns including possible layering schemes, transactions not commensurate with the business's purpose, and commingling of funds between two independent check cashing entities. Merchants's leadership impeded BSA analysts and other employees investigating activity on transactions associated with accounts that were affiliated with Bank executives, and the activity in these accounts went unreported for many years. Employees who attempted to report suspicious activity in these accounts were threatened

[8] 31 U.S.C. §§ 5318(a)(2), 5318(h)(1); 31 C.F.R. § 1020.210; 12 C.F.R. § 21.21.

[9] 31 U.S.C. § 5318(h)(1)(A); 31 C.F.R. § 1020.210.

with possible dismissal or retaliation. Merchants's executives weakened the Bank's AML program by creating a culture that did not sufficiently detect or report on suspicious activity involving the accounts of insiders.

a. Due Diligence for High-risk MSB customers

Merchants failed to adopt and implement adequate policies and procedures to conduct required due diligence for its large portfolio of high-risk MSB customers. Considering these customers and services, risk-based due diligence assessments were necessary to assist the Bank in determining when transactions were potentially suspicious and enable reporting of those transactions as required by the BSA.

Merchants failed to collect the information necessary to establish sufficient knowledge of its MSB customers' activities. Merchants provided banking services to a large number of MSB customers, the vast majority of which were considered high-risk. Merchants's customer application forms did not provide for the sufficient documentation of customers' anticipated account activity. In addition, Merchants did not have procedures for identifying the source of funds for its high-risk MSB customers. For example, one of these customers owned check-cashing businesses located along the Mexican border, which increased the possibility that its source of funds came from Mexico. Despite this, Merchants did not sufficiently monitor or analyze this account activity, nor did it conduct any due diligence to identify the source of funds for the MSB's check cashing businesses. The Bank also failed to conduct account reviews of its high-risk MSB customers, particularly for MSB customers located hundreds of miles away from its community bank-designated location.

Merchants failed to implement a due diligence program that would mitigate the money laundering risks of its higher risk services and customers, including MSBs located hundreds of

miles from the Bank. Merchants's MSB program was critically deficient in both its review and verification of customer information and in its processes for ongoing monitoring of customer activity. Merchants did not adequately review and verify information it received from high-risk customers. By not implementing reasonable procedures to review and verify the information provided by its customers, Merchants failed to collect sufficient information and identify effective measures to monitor its accounts for suspicious transactions. For example, Merchants maintained an account for a specific MSB, which stated that the purpose for its account was to support check-cashing operations at three locations in Puerto Rico. However, this MSB was also using the account to make deposits from its remittance activities associated with another MSB. Merchants did not compare this account activity with its originally stated purpose in order to assess the change in its customer's risk profile. Merchants failed to identify the sources of funds and failed to detect and report suspicious activity related to the commingled transactions. The risks inherent in a customer providing money transmission are different and require different mitigating procedures than for a customer that only serves as a check casher. Merchants's failures in conducting due diligence on this account prevented the Bank from assessing the money laundering risk related to its customer's commingled transactions.

Prior to September 2016, Merchants failed to adequately monitor the activity of its higher-risk customers. Merchants had over 165 check cashing customers that required large volumes of cash. Considering that cash is the most commonly used instrument to launder money, Merchants should have assessed its MSB customers' cash flows by reviewing them periodically, identifying their sources of funds, documenting expected account behavior, and maintaining awareness of each MSB's customer base. Merchants did not perform sufficient account cash flow analysis to monitor the ways MSB customers were funding their check

cashing operations. Many of Merchants's MSB customers commingled funds in the same accounts. This reduced the transparency of the transactions and hampered the Bank's ability to determine the source of funds. Consequently, Merchants did not detect or analyze the shortfalls in funding for check cashing activities nor identify alternative funding sources, which may have included cash inflows from remittance activities. Merchants did not adequately evaluate and identify suspicious activity related to these commingled transactions.

b. Risk Management of Remote Deposit Capture Services

Until 2016, Merchants failed to adequately implement internal controls to mitigate the risks of the RDC services that it offered to high-risk MSBs located hundreds of miles from its location. Merchants was required to evaluate the risks and regulatory requirements when implementing RDC services and to have adequate policies and procedures in place to manage these risks and ensure monitoring systems were set up to adequately detect suspicious transactions. Merchants did not have the overall infrastructure necessary to routinely monitor the scope of its RDC activities deployed to MSB customers, and therefore failed to mitigate the risks that its RDC services posed to the Bank. Merchants provided its MSB customers with RDC services without establishing sufficiently tailored customer risk-rating categories and policies for monitoring this activity. Prior to September 2016, Merchants continued to provide RDC services to MSBs without ensuring the legitimacy of the MSBs' source of funds, conducting transaction monitoring, or documenting and reviewing account alerts.

2. Independent Testing

Until 2015, Merchants failed to conduct an independent audit that was commensurate with the Bank's customer complexity and risk profile. Merchants is required to conduct independent compliance testing commensurate with the BSA/AML risk profile of the Bank to

monitor and maintain an adequate program.[10] By not conducting the required independent review, Merchants was unable to identify vulnerabilities in its compliance program and properly monitor the account activity of its customers to detect suspicious activity going through the Bank.

Merchants failed to have proper requirements within the Bank's AML program to ensure that the audit firm conducted a comprehensive independent audit of its program. Specifically, Merchants failed to adequately review the engagement proposal of the audit firm to confirm it was sufficient in scope to identify weaknesses in the Bank's program.

Merchants's independent audit was not commensurate to the risk and complexity of the types of customers Merchants served, including its high-risk MSB customers. Therefore the 2012 independent audit failed to identify internal control deficiencies in Merchants's AML program. The audit's scope, procedures, and transaction review of Merchants's independent testing were inadequate, given the Bank's high-risk customer base. In 2014, a new independent consultant conducted an audit but failed to identify significant gaps in Merchants's overall BSA compliance program. In 2015, Merchants hired a different independent consultant only to conduct a required SAR look-back review of the Bank's MSB account activity. During this review, the consultant identified a number of AML compliance issues that Merchants's former auditors failed to identify. The consultant identified issues that were consistent with Merchants's internal controls violations related to providing banking services to high-risk MSBs without implementing the appropriate risk-based controls required by the BSA or creating an appropriate due diligence program.

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

3. Designation of a BSA Compliance Officer

Merchants failed to provide the necessary level of authority, independence and responsibility to its BSA Officer to ensure day-to-day compliance with the BSA as required.[11] Merchants's BSA Officer and the compliance staff were not empowered with sufficient authority and autonomy to implement the Bank's AML program. Merchants's interest in revenue compromised efforts to effectively manage and mitigate its deficiencies and risks.

Prior to September 2016, Merchants's leadership had not ensured that the BSA Officer had sufficient authority and resources to administer an effective BSA compliance program by failing to define a permanent BSA department structure and to establish criteria regarding how the BSA Officer roles and responsibilities would successfully be performed. Specifically, the BSA department had relied on other departments within the Bank to make determinations on acceptable risks often without clear guidance from the BSA department. For those BSA responsibilities for which other departments did have specific guidelines, including the collection of customer information, there was no accountability when those departments failed to abide by the AML program. At Merchants, BSA duties were shared among other departments at the Bank, including those associated with specific business lines, where its staff lacked BSA knowledge and experience.

From August 2014 to April 2015, Merchants failed to designate a BSA Officer and had three people sharing the BSA Officer duties without clearly defining each individual's responsibility. The staff assigned these responsibilities were neither BSA knowledgeable nor adequately trained in their BSA duties. Most concerning was the fact that two out of these three individuals were Merchants's executives in charge of bringing businesses to the Bank,

[11] 31 U.S.C. § 5318(h)(1)(B); 31 C.F.R. § 1020.210.

particularly MSBs, creating a conflict of interest that impeded them from performing compliance duties on their own customers.

Merchants's leadership did not provide the BSA department with the appropriate level of authority, autonomy, or independence in which to properly and effectively execute its responsibilities to ensure the Bank's compliance with the BSA. For example, despite repeated recommendations to improve its AML program, Merchants continuously failed to establish clear policies for correcting key BSA/AML deficiencies.

From 2009 to September 2016, Merchants did not establish an effective process to ensure management could effectively address adverse findings in compliance reviews. Specifically, the Bank had inadequate policies and procedures to implement corrective actions for its BSA/AML program deficiencies. Because of these failures, Merchants maintained an AML program with repeated, material deficiencies in its risk identification and assessment, controls to mitigate risk, monitoring for suspicious transactions, and collecting sufficient account documentation.

4. Training

Merchants's BSA/AML training program was not commensurate with the Bank's customer risk profile and services offered. A bank's AML program must provide for education and training of personnel regarding its responsibilities under the program, including the detection of suspicious transactions.[12] Merchants's training program consistently failed to provide BSA staff with adequate job-specific training. The Bank's training program focused only on general BSA/AML requirements and did not include topics on risks specific to the Bank. As a result, Merchants's employees did not have training specific to their positions, which is necessary to recognize suspicious activity when monitoring the transactions of high-risk MSBs.

[12] 31 U.S.C. § 5318(h)(1)(C); 31 C.F.R. § 1020.210.

Merchants's failure to institute a training program that adequately addressed BSA issues and risks specific to the Bank contributed to the Bank's failure to identify and report suspicious activity of high-risk MSB customers.

B. Due Diligence Program for Correspondent Accounts for Foreign Financial Institutions

From 2008 to 2014, Merchants failed to maintain a due diligence program for foreign correspondent accounts. Foreign correspondent accounts are gateways to the U.S. financial system. U.S. banks maintaining correspondent accounts in the United States for foreign financial institutions must subject the accounts and respondents to certain due diligence measures as part of their AML obligations.[13]

Merchants failed to identify and perform adequate due diligence on its foreign correspondent banking customers. One of the central goals of the USA PATRIOT Act is to protect access to the U.S. financial system by requiring certain records, reports, and due diligence programs for foreign correspondent accounts. The Bank did not have policies and procedures to elevate foreign correspondent bank customers for enhanced due diligence, as required in section 312 of the USA PATRIOT Act. Merchants failed to identify foreign financial institutions as foreign correspondent accounts. For example, Merchants had four banking customers located in several jurisdictions considered to be high-risk including Honduras, Mexico, Colombia, and Romania but did not identify these customers as foreign correspondent customers, and therefore did not implement the required customer due diligence program. These four customers sent and received a combined $192 million in high-risk wire transfers during the period of August 2014 through October 2014. Merchants failed to establish adequate alert

[13] 31 U.S.C. § 5318(i)(1); 31 C.F.R. 1010.610.

parameters for these accounts, resulting in the exclusion of this wire activity from monthly transactional monitoring because the Bank failed to establish appropriate alert parameters on the accounts. Merchants failed to identify suspicious wires and report that activity to FinCEN during this time.

C. Violations of the Requirement to Report Suspicious Transactions

The BSA and its implementing regulations impose an obligation on banks to report transactions that involve or aggregate to at least $5,000, 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 sort in which the customer normally would be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction.[15]

From 2012 to 2016, Merchants failed to adequately monitor billions of dollars of transactions for suspicious activity. Because of this failure, Merchants failed to file or file timely on hundreds of millions of dollars of suspicious activity including millions of dollars of transactions of 57 of its customers later identified as part of an independent look-back review.

Many of Merchants failures to file or file timely SARs were related to its higher-risk MSB customers' activities, which were inconsistent with the anticipated behavior, stated business purpose, or customer profile information of these MSBs. For example, one of the MSB

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

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

customers was a money transmitter located in the basement of the owner's private residence in New York. Despite several red flags resulting from Merchants's account review, including the fact that this MSB was the subject of multiple information requests from law enforcement, had significant increases in its account activity, and its wire transfers were, in two instances, rejected by another bank, Merchants determined that its activities were not suspicious and failed to timely file a SAR.

Merchants also failed to file a SAR on another MSB customer engaging in suspicious activity. In a six-month period between 2011 and 2012, the MSB conducted approximately $500,000 and $700,000 in deposits and withdrawals, respectively, and received over $1.3 million in wire transfers. Within two to three days of receiving the funds, the MSB wrote large checks, cashing them out at other financial institutions. In January 2012, Merchants conducted a due diligence analysis on the same MSB's activity and did not consider it suspicious. In February 2012, after learning of a criminal investigation involving the MSB, Merchants again conducted a due diligence analysis and again failed to report the customer and its activity in a SAR. On September 19, 2012, the MSB and its manager pleaded guilty to eight counts of failing to file currency transaction reports and one count of failing to maintain an effective AML program.

In addition, Merchants failed to file a SAR on another licensed money transmitter and seller of money orders with physical locations in Nevada and California. This MSB's customer base was located in Russia, Armenia, the United Kingdom, and Germany, and the MSB sent most of its money transmissions to these regions. Merchants rated this account as high-risk and conducted an account review, which indicated that for several months, the volume of account activity had significantly exceeded the anticipated activity established by the MSB during the account application process. Although the review indicated that Merchants asked the MSB for

an explanation of its unexpected account behavior, the customer never provided the requested information and the Bank failed to investigate further. Merchants also failed to identify evidence of structuring flowing through the account.

In 2015, an independent consultant completed a look-back review of a sample of 100 of Merchants's high-risk MSB accounts for the period of July 1, 2012 through June 30, 2014. The look-back review identified 57 customer accounts with activity that was deemed potentially suspicious and required escalation to management level along with an additional 11 customer accounts requiring further review due to a lack of documentation or a lack of transparency in the customer transactions. The independent consultant identified weaknesses in Merchants's AML program consistent with the Bank's internal controls violations, which led to Merchants's failure to report suspicious activity.

As a result of the look-back review, Merchants filed SARs on the activity and transactions identified through the review. The late SAR filings included reports covering structured transactions that were conducted through Merchants for two consecutive years totaling over $400 million. The subjects of one of the SARs engaged in a suspicious pattern of cashing multiple structured checks made to the order of the same individuals in Mexico without providing information concerning source of funds. Also, these subjects engaged in several suspicious wire transfers to the Office of Foreign Assets Control sanctioned countries. These same subjects were under a U.S. federal law enforcement investigation for fraudulent tax returns. This activity started in 2014 and was reported on a SAR two years later only after Merchants was required to conduct a look-back review.

Another late SAR covered transactions worth over $395 million related to customers conducting large wire transfers between multiple foreign financial institutions without validating

the source of funds or identifying the ultimate beneficiary. This activity resulted in large payouts to unknown entities in Colombia.

Merchants's failure to conduct sufficient due diligence investigations on MSB accounts led to its failure to file multiple SARs.

III. CIVIL MONEY PENALTY

FinCEN has determined that Merchants willfully violated the AML program, reporting, and recordkeeping requirements of the BSA and its implementing regulations as described in the CONSENT, and that grounds exist to assess a civil money penalty for these violations.[16]

FinCEN has determined that the penalty in this matter will be $7 million. The penalty will run concurrent with the OCC's $1 million penalty.

IV. CONSENT TO ASSESSMENT

To resolve this matter, and only for that purpose, Merchants consents to this ASSESSMENT of a civil money penalty in the sum of $7 million and admits that it willfully violated the BSA's program, recordkeeping, and reporting requirements.

Merchants recognizes and states that it enters into the CONSENT freely and voluntarily and that no offers, promises, or inducements of any nature whatsoever have been made by FinCEN or any employee, agent, or representative of FinCEN to induce Merchants to enter into the CONSENT, except for those specified in the CONSENT.

Merchants understands and agrees that the CONSENT embodies the entire agreement between Merchants and FinCEN relating to this enforcement matter only, as described in Section II above. Merchants further understands and agrees that there are no express or implied promises, representations, or agreements between Merchants and FinCEN other than those

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

expressly set forth or referred to in this document and that nothing in the CONSENT or in this ASSESSMENT is binding on any other agency of government, whether Federal, State or local.

V. PUBLIC STATEMENTS

Merchants expressly agrees that it shall not, nor shall its attorneys, agents, partners, directors, officers, employees, affiliates, or any other person authorized to speak on its behalf, make any public statement contradicting either its acceptance of responsibility set forth in the CONSENT or any fact in the DETERMINATIONS section of the CONSENT. FinCEN has sole discretion to determine whether a statement is contradictory and violates the terms of the CONSENT. If Merchants, or anyone claiming to speak on behalf of Merchants, makes such a contradictory statement, Merchants may avoid a breach of the agreement by repudiating such statement within 48 hours of notification by FinCEN. If FinCEN determines that Merchants did not satisfactorily repudiate such statement(s) within 48 hours of notification, FinCEN may void, in its sole discretion, the releases contained in the CONSENT and reinstitute enforcement proceedings against Merchants. Merchants expressly agrees to waive any statute of limitations defense to the reinstituted enforcement proceedings and further agrees not to contest any admission or other findings made in the CONSENT. This paragraph does not apply to any statement made by any present or former officer, director, employee, or agent of Merchants in the course of any criminal, regulatory, or civil case initiated against such individual, unless Merchants later ratifies such claims, directly or indirectly. Merchants further agrees that, upon notification by FinCEN, it will repudiate such statement to the extent it contradicts either its acceptance of responsibility or any fact in the CONSENT.

VI. RELEASE

Execution of the CONSENT, upon it being effective, and compliance with all of the terms of this ASSESSMENT and the CONSENT, settles all claims that FinCEN may have against Merchants for the conduct described in Section II of the CONSENT. Execution of the CONSENT, and compliance with the terms of this ASSESSMENT and the CONSENT, does not release any claim that FinCEN may have for conduct by Merchants other than the conduct described in Section II of the CONSENT, or any claim that FinCEN may have against any current or former director, officer, owner, or employee of Merchants, or any party other than those named in the CONSENT. Upon request, Merchants shall truthfully disclose to FinCEN all factual information not protected by a valid claim of attorney-client privilege or work product doctrine with respect to the conduct of its current or former directors, officers, employees, agents, or others.

By:

/s/ 2/16/17

Jamal El-Hindi Date:
Acting Director
FINANCIAL CRIMES ENFORCEMENT NETWORK (FinCEN)
U.S. Department of the Treasury