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

IN THE MATTER OF:	)	
	)	
	)	
	)	**Number 2014-07**
North Dade Community Development	)	
Federal Credit Union	)	
Miami Gardens, Florida	)	

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 North Dade Community Development Federal Credit Union ("North Dade") pursuant to the Bank Secrecy Act ("BSA") and regulations issued pursuant to that Act.[1]

North Dade admits to the facts set forth below and that its conduct violated the BSA. North Dade consents to the assessment of a civil money penalty and enters 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.

[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.

FinCEN has the authority to investigate credit unions for compliance with and violation of the Bank Secrecy Act pursuant to 31 C.F.R. § 1010.810, which grants FinCEN "[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." North Dade was a "financial institution" and a "bank" within the meaning of the BSA and its implementing regulations during the time relevant to this action. 31 U.S.C. § 5312(a)(2)(E); 31 C.F.R. §§ 1010.100(d)(6), 1010.100(t)(1).

North Dade is a non-profit, federally chartered, community development financial institution located in Miami Gardens, Florida. The National Credit Union Administration ("NCUA") is North Dade's federal functional regulator and examines credit unions, including North Dade, for compliance with the BSA and its implementing regulations. North Dade was founded in 1997 to serve the North Dade/Broward County community area. Credit unions have authorized fields of membership, which means that a limited group of people and entities are eligible to be members of the credit union. North Dade's authorized field of membership is limited to individuals and entities that live, work, or worship in the North Dade County area. North Dade has one branch, with five employees, and assets of $4.1 million dollars.

North Dade's BSA failures derived significantly from its banking services to certain money services businesses ("MSBs"). These MSBs were located outside of its geographic field of membership and were engaged in high-risk activities, such as wiring millions of dollars per month to high-risk foreign jurisdictions. For instance, in 2013 alone, the total transaction volume through North Dade by MSBs included $54.8 million in cash orders, $1.01 billion in

outgoing wires, $5.3 million in returned checks, and $984.4 million in remote deposit capture.[2] North Dade's MSB activity accounted for 90% of North Dade's total annual revenue in 2013. This was not the expected business behavior of a small credit union like North Dade and led to substantial BSA compliance failures and violations.

II. DETERMINATIONS

FinCEN has conducted an investigation and determined that, from December 2009 through January 2014, North Dade willfully violated the BSA's program, reporting, and recordkeeping requirements.[3] NCUA cited North Dade for many of these violations in a Cease and Desist Order issued on September 6, 2013.

As described in more detail below, North Dade: (a) failed to implement an adequate anti-money laundering program, 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210; (b) failed to develop and implement an adequate customer identification program, 31 U.S.C. § 5318(l); 31 C.F.R. § 1020.220; (c) failed to detect and adequately report suspicious transactions, 31 U.S.C. § 5318(g); 31 CFR § 1020.320; and (d) failed to access or review FinCEN's 314(a) lists, 31 CFR § 1010.520.

---

[2] Remote Deposit Capture allows financial institution customers to "deposit" checks electronically at remote locations, usually in the customers' offices, for virtually instant credit to their account. Paper checks are digitally scanned, and an image of the check is electronically transmitted to the customer's bank.

[3] In civil enforcement of the Bank Secrecy Act 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 Bank Secrecy Act, or that the entity or individual otherwise acted with an improper motive or bad purpose. North Dade admits to "willfulness" only as the term is used in civil enforcement of the Bank Secrecy Act under 31 U.S.C. § 5321(a)(1).

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

North Dade failed to establish and implement an effective anti-money laundering compliance program. The BSA and its implementing regulations require all federally chartered credit unions to establish and implement anti-money laundering programs. 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210. NCUA requires each federally chartered credit union to develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements of the BSA, including an appropriate customer identification program. 12 C.F.R. § 748.2(b); 31 C.F.R. § 1020.220(a)(1).

North Dade failed to establish and maintain an adequate written compliance program that, at a minimum: (1) provided for a system of internal controls to assure ongoing compliance; (2) provided for independent testing for compliance to be conducted by bank personnel or by an outside party; (3) designated an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (4) provided training for appropriate personnel. 31 U.S.C. § 5318(h)(1); 31 C.F.R. § 1020.210; 12 C.F.R. § 748.2(c). North Dade's compliance program also did not include a customer identification program that was appropriate for its size and type of business. 31 U.S.C. § 5318(l); 31 C.F.R. § 1020.220(a)(1); 12 C.F.R. § 748.2(b)(2).

1. Internal Controls

North Dade failed to implement an effective system of internal controls reasonably designed to ensure compliance with the BSA. It did not timely assess its own money laundering and terrorist financing risks or design an anti-money laundering compliance program to address those risks. As a result, North Dade served a large number of high-risk MSBs outside of its field of membership without exercising adequate compliance oversight.

Risk Assessment

North Dade did not perform a risk assessment until November 2013. A risk assessment is a vital part of a compliance program, as it permits the financial institution to assess its particular risks given its business lines, practices, and clientele and design a program that can reasonably assure and monitor BSA compliance given those risks. North Dade failed to assess the risks of its business lines between December 2009 and November 2013. When NCUA examiners requested a copy of North Dade's risk assessment for its December 31, 2011 exam, they were provided with an outdated template from the 2006 Federal Financial Institutions Examination Council Manual rather than an assessment of North Dade's particular risks. While North Dade had independent audits that identified money laundering and terrorist financing risks in 2012, it did not complete a risk assessment until November 2013. Because North Dade did not examine the services it provided and evaluate the money laundering and terrorist financing risks presented by those services, given North Dade's location, customers, services offered, size, and volume of business, North Dade was ill-equipped to develop a compliance program that included appropriate processes and procedures to address those specific risks and identify suspicious activity.

Risk-Based Procedures to Ensure Compliance

North Dade had insufficient internal controls to identify and monitor suspicious activity taking place through the credit union, in part because it did not assess its own risks and implement procedures designed to address those unique risks. This internal control failure was particularly evident in its generally higher-risk MSB business lines. The most significant example of North Dade's failure to have adequate internal controls and an adequate compliance program is its MSB contract with a third-party vendor.

In December 2009, North Dade entered into a contract with a third-party vendor ("the Vendor"), itself an MSB, to provide financial services to other MSBs, including check-cashing stores and currency exchangers. North Dade agreed to become the depository institution for the Vendor's MSB clients, providing sub-accounts for each MSB to conduct deposits and transfer funds. Under the contract, the Vendor was North Dade's member and customer and the Vendor's MSB clients were not. However, in practice, 56 of the Vendor's MSBs sub-accounts could receive financial services directly from North Dade. In either case, North Dade had anti-money laundering compliance responsibilities with which it did not comply. For example, North Dade's own counsel advised that, although it could open this type of account, North Dade would still have anti-money laundering compliance responsibilities for the Vendor's MSBs. These responsibilities included a customer identification program and other required due diligence on the MSBs and their transactions. Likewise, to the extent opening accounts gave North Dade a direct relationship with the Vendor's MSBs, North Dade would have the same anti-money laundering obligations as it would for any member.

The revenue generated by this business line was vital to North Dade's survival. At one point, the Vendor's MSBs accounted for 90% of North Dade's total annual revenue. The substantial revenue generated by the Vendor's program appeared to outweigh any consideration by North Dade of associated risks and appropriate compliance measures. For example, NCUA examined North Dade in 2010 and instructed the credit union to ensure that its MSB members all met field of membership requirements. But, by December 2012, North Dade had accounts for 56 different MSBs under its Vendor contract that were located outside of North Dade's field of membership. Many of these MSBs were located in jurisdictions in the Middle East and Central America that pose a significant money laundering risk. In addition, despite acknowledging that

it had anti-money laundering compliance responsibilities for these high-risk accounts, North Dade relied on the Vendor to conduct all related due diligence and suspicious activity monitoring without conducting any verification or inspection of the Vendor's compliance activities. Further, North Dade did not verify the customer identification information on the MSBs that the Vendor provided to North Dade.

North Dade did not have sufficient policies and procedures to ensure compliance. Until it instituted a new anti-money laundering policy in November 2013, it lacked: (1) written procedures for opening accounts for members who did not have a social security or tax identification number; (2) written procedures to follow up with account holders whose files were missing social security or tax identification numbers; (3) procedures to ensure that potential high-risk accounts were properly rated as to their money laundering risk; (4) adequate procedures for monitoring accounts for both particular incidents as well as ongoing patterns of suspicious activity; and (5) procedures to retain supporting documentation for filed suspicious activity reports and copies of currency transaction reports.

North Dade's five-person staff did not have sufficient resources or technical expertise to administer a program capable of ensuring compliance with the BSA. North Dade lacked sufficient numbers and expertise in its staff and an adequate technical infrastructure to create, implement, and maintain an anti-money laundering program sufficient to monitor and report on high-volume, high-risk business lines and customers, such as some of the MSBs in the Vendor's contract. As discussed below, North Dade did not provide sufficient training to ensure that its staff had the skills necessary to administer a program to monitor a large number of high-risk customers and transactions, and did not timely obtain the outside assistance or technical resources to compensate for its small staff.

North Dade also did not implement appropriate procedures to manage its customers' compliance risk, given that many of the Vendor's MSBs engaged in particularly high-risk activities, including high-risk currency exchanges. North Dade handled large international transactions for the MSBs. For example, these transactions included, during a one-year period, (1) deposits in excess of $14 million in U.S. cash that was physically imported into the United States on behalf of nearly 40 Mexican currency exchangers, and (2) hundreds of millions of dollars in wire transfers to foreign bank accounts of MSBs located in Mexico and Israel.

Despite these high-risk activities, North Dade did not have any risk or transaction tracking criteria or other compliance procedures to identify and manage high-risk accounts and transactions and instead improperly relied upon the Vendor's compliance activities. For example, one individual, connected to over 60% of the businesses banking with North Dade, conducted transactions between January 2010 and August 2013, that resulted in 2,036 currency transaction reports being filed for cash withdrawals. However, North Dade never identified this customer as being potentially high-risk or reviewed his activities. Because North Dade did not have appropriate policies and procedures in place to identify and monitor high-risk customers and services, numerous suspicious transactions flowed through North Dade accounts without North Dade reviewing them and, when appropriate, filing suspicious activity reports. These suspicious transactions, based on available information, potentially involved money laundering, evasions of Mexican currency transaction restrictions, and drug trafficking.

North Dade failed to have an effective suspicious activity monitoring system for its customers, particularly the Vendor's MSB customers. North Dade relied completely on the Vendor to monitor its MSBs' transactions. In addition, North Dade had insufficient procedures in place to detect suspicious activity among its member customers in general until sometime after

its audit report in August 2013. That report detailed North Dade's inadequate suspicious transaction monitoring procedures and automated systems. In order to monitor for suspicious activities, employees had to manually investigate accounts. However, North Dade's small number of employees lacked the BSA experience, knowledge, and skills to conduct such monitoring, there was an insufficient number of staff to manually review the volume of transactions North Dade was conducting, and North Dade did not implement an appropriate training program to help mitigate this problem. Because of North Dade's failure to appropriately monitor transactions and file SARs for several years, suspicious activity may have gone unnoticed and unreported.

North Dade also did not fully implement the internal controls it did have to ensure BSA compliance. In addition to the Vendor's MSBs, North Dade provided banking services to other MSBs. North Dade's internal policy required each MSB to be properly registered with FinCEN and properly licensed with the state in which they are conducting businesses. In the event that the MSB was not properly registered and licensed, North Dade's written policy was to deny further services to that member. Despite this policy, North Dade continued to provide services to MSBs located in the Middle East, well outside its field of membership, that were not registered with FinCEN.

North Dade failed to assess its money laundering and terrorist financing risks, design appropriate policies and procedures to ensure BSA compliance given those risks, identify customers and monitor their account activities given the customer's level of money laundering risk, and monitor for both individual incidents and ongoing patterns of suspicious activity. North Dade's compliance program was therefore not reasonably designed to ensure BSA compliance.

2. Designation of BSA Compliance Officer

A federally chartered credit union is required to designate a person responsible for ensuring day to day compliance with BSA requirements. 31 C.F.R. § 1020.210; 12 C.F.R. § 748.2(c). North Dade failed to designate a person responsible to oversee BSA compliance, and no staff member was otherwise assigned or technically competent to oversee ongoing compliance efforts. This compliance violation was highlighted during an independent testing review conducted in 2011. While North Dade repeatedly indicated that it would correct this issue, it failed to designate a compliance officer until January 2014, three years later.

3. Training

A federally chartered credit union's anti-money laundering program must provide for education and training of personnel regarding its responsibilities under the program, including the detection of suspicious transactions. 31 C.F.R. § 1020.210; 12 C.F.R. § 748.2(c). North Dade did not have any records of BSA and anti-money laundering compliance for its Board of Directors as recommended by the Federal Financial Institutions Examination Council Manual. North Dade's employees did receive annual BSA training. The training provided, however, was significantly deficient because it (1) did not encompass all aspects of BSA; (2) was not tailored for each department; (3) did not provide sufficient references to external sources to ensure that employees had access to current information on BSA compliance rules and guidance; and (4) did not cover compliance for MSB customers and accounts. Because the training omitted information on MSB compliance and risks, North Dade staff did not have guidance to understand the risks associated with the credit union's largest volume of transactions or how to adequately monitor them.

4. Independent Testing

A federally chartered credit union's anti-money laundering program must include independent compliance testing to monitor the institution's program and ensure its adequacy. 31 C.F.R. § 1020.210; 12 C.F.R. § 748.2(c). NCUA recommends annual testing of a credit union's compliance program when it serves high-risk clients. North Dade did not have its anti-money laundering program tested on a regular basis until NCUA cited this shortfall, a failure of particular concern for an entity, like North Dade, engaged in high-risk business lines. North Dade began receiving independent audits in December 2011 and began addressing some of the programmatic deficiencies shortly thereafter. However, many significant issues persisted almost two years later. North Dade's August 2013 independent audit identified a number of continuing deficiencies, including inadequate suspicious activity monitoring, failing to file timely suspicious activity and currency transaction reports, maintaining accounts for MSBs located outside of North Dade's field of membership, and failing to have procedures to ensure that all required due diligence is performed when new accounts are opened.

B. Customer Identification Program

As part of its anti-money laundering compliance program, a credit union must implement a written Customer Identification Program ("CIP") appropriate for its size and type of business. The program must include risk-based identity verification, recordkeeping, and retention procedures, as well as procedures to determine whether an account is being opened for a government-designated terrorist or terrorist organization and to take appropriate follow-up action if a customer is designated. 31 U.S.C. § 5318(l); 31 C.F.R §§ 1020.210, 1020.220; 12 C.F.R. § 748.2(b)(2). CIP helps a financial institution determine the risks posed by a particular customer, allowing the institution to ensure that it has the proper controls in place, including

suspicious activity monitoring procedures, and to monitor and report on the risks of a particular client.

In relation to the Vendor's MSB clients, North Dade had no procedures in place to address CIP requirements. While North Dade management discussed the high risk posed by this business line as early as March 2010, North Dade's staff and management never reviewed, researched, or verified the identities of the holders of any of the MSB accounts. Instead, North Dade relied exclusively on the Vendor to perform CIP functions. A credit union may rely on another financial institution only in instances where the credit union and the financial institution share customers, and the financial institution is regulated by a federal functional regulator. 31 C.F.R. § 1020.220(a)(6).[4] In this case, North Dade should not have relied on the Vendor for CIP compliance because, as an MSB, the Vendor was not regulated by a federal functional regulator. By not knowing its members, North Dade was not capable of understanding their expected transactional behavior and thus was unable to appropriately monitor for suspicious activities.

C. <u>Suspicious Activity Reporting Violations</u>

The Bank Secrecy Act and its implementing regulations impose an obligation on financial institutions to report transactions that involve or aggregate to at least $5,000; are conducted by, at, or through the financial institution; and that the institution "knows, suspects, or has reason to suspect" are suspicious. 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320(a)(2). A transaction is "suspicious" if the transaction: (1) involves funds derived from illegal activities,

---

[4] See also *Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act,* Financial Crimes Enforcement Network, et al. (April 28, 2005), available at http://www.fincen.gov/statutes_regs/guidance/pdf/faqsfinalciprule.pdf.

or is conducted to disguise funds derived from illegal activities; (2) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations under the BSA; or (3) has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction. 31 C.F.R. § 1020.320(a)(2). North Dade failed to detect and timely report suspicious activity.

Between April 2010 and April 2013, North Dade filed only 15 Suspicious Activity Reports ("SARs"). The SARs were filed late and the narrative sections lacked essential information explaining why the suspicious activity was being reported. Furthermore, North Dade failed to file SARs on customers engaged in suspicious activity, including a customer that was arrested and charged with conspiring to launder money. Law enforcement seized more than $1.5 million dollars from an owner of an MSB who held an account at North Dade, yet North Dade never filed a SAR on the MSB or its owner.

D. Section 314(a) of the USA PATRIOT Act

Section 314(a) of the USA PATRIOT Act and its implementing regulations authorize a federal law enforcement agency investigating terrorist activity or money laundering to request that FinCEN solicit, on the agency's behalf, certain information from financial institutions regarding subjects of interest in bona fide law enforcement investigations. Financial institutions are required to review and respond as appropriate to requests from FinCEN on behalf of law enforcement for information relating to individuals, entities, or organizations engaged in, or reasonably suspected based on credible evidence of engaging in, terrorist activity or money laundering. Upon receiving an information request from FinCEN under this section, a financial

institution must expeditiously search its records to determine whether it maintains or has maintained an account for, or has engaged in a transaction with, each individual, entity, or organization named in the request. The 314(a) process provides an important expedited communication system that allows law enforcement to rapidly obtain and evaluate potential lead information in significant and often time-sensitive money laundering and terrorist financing investigations. 31 C.F.R. § 1010.520.[5]

North Dade failed to comply with its Section 314(a) obligations by failing to access or review FinCEN's 314(a) lists from 2012 through 2013. The lists are posted by FinCEN on a secure website every two weeks and must be downloaded and responses verified by the financial institution within a specified deadline. During 2012, the North Dade did not review the list on fourteen of the posted requests and reviewed five requests late. In addition, North Dade had the 314(a) requests sent to a single email address that was accessed by only one person, making timely responses dependent on that person's availability.

III. CIVIL MONEY PENALTY

FinCEN has determined that North Dade willfully violated the program, reporting, and recordkeeping requirements of the Bank Secrecy Act and its implementing regulations, as described in this ASSESSMENT, and that grounds exist to assess a civil money penalty for these violations. 31 U.S.C. § 5321 and 31 C.F.R. § 1010.820. FinCEN has determined that the penalty in this matter will be $300,000.

---

[5] *See also Fincen's 314(a) Fact Sheet* (August 19, 2014), available at http://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf.

IV. CONSENT TO ASSESSMENT

To resolve this matter, and only for that purpose, North Dade consents to the assessment of a civil money penalty in the sum of $300,000, and admits that it violated the BSA's program, recordkeeping, reporting and requirements.

North Dade 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 North Dade to enter into the CONSENT, except for those specified in the CONSENT.

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

Execution of the CONSENT, and compliance with all of the terms of this ASSESSMENT and the CONSENT, settles all claims that FinCEN may have against North Dade 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 North Dade other than the conduct described in Section II of the CONSENT, or any claim that FinCEN may have against any director, officer, owner, employee, or agent of North Dade, or any party other than North Dade. Upon request, North Dade 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/ November 25, 2014

Jennifer Shasky Calvery Date:
Director
FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. Department of the Treasury