Steptoe

INTERNATIONAL LAW ADVISORY

FinCEN Penalizes Compliance Officer for Anti-Money Laundering Failures

March 24, 2020

Authors

M. Jeffrey Beatrice, Zoe Osborne, Jack R. Hayes, Nicholas Turner, Jillian Norton

Overview

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

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

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

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

The Civil Money Penalty

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

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

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

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

Failure to Ensure Sufficient AML Resources

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

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

LaFontaine's Role in SARs Failures

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

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

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

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

Compliance Takeaways

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

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

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

2. Ensure Technology is Appropriately Calibrated to Flag Suspicious Activity

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

3. Escalate Internal Warnings

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

4. Take Heed from Other Enforcement Actions

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

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

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

Practices

Anti-Money Laundering

Independent & Internal Investigations

FCPA/Anti-Corruption

Financial Services