



A Cautionary Tale for Money Service Businesses: How Violating the Bank Secrecy Act Could Cost Millions

Mar 02, 2017

Categories:

[Blockchain and Digital](#)

[Assets](#)

[Blogs](#)

[Publications](#)

Authors:

[William T. Repasky](#)

On February 27, 2017, The Financial Crimes Enforcement Network (“FinCEN”) fined Merchants Bank of California (“Merchants”) \$7 million for what it called “egregious” violations of the Bank Secrecy Act (“BSA”). The Office of the Comptroller of the Currency simultaneously assessed a \$1 million civil monetary penalty against Merchants because it violated two previous consent orders. Merchants is a community bank located in Carson City, California. The Bank had a large portfolio of Money Service Businesses (“MSBs”) customers. MSBs are generally recognized by federal regulators to include: (1) currency dealers or exchangers; (2) check cashers; (3) issuers of traveler’s checks, money orders, or stored value; (4) sellers or redeemers of traveler’s checks, money orders, or stored value; and (5) money transmitters. In Merchants’ case, it had 165 check-cashing and 44 money-transmitter customers, who often operated at great distances from the Bank. Compounding the situation was the fact that Bank insiders owned or managed a number of the MSB customers.

In finding that Merchants “willfully” violated the BSA, FinCEN focused on Merchants’ failures to establish and implement an appropriate Anti-Money Laundering (“AML”) program, to conduct due diligence on its foreign correspondent accounts, and to report suspicious activity. The case illustrates how even down-stream misconduct of third party actors, like MSBs, can cost financial institutions millions in BSA civil penalties. Failure to adhere to the BSA hygiene may result in substantial civil monetary penalties or, even worse, a prison sentence.

FinCEN found that Merchants failed to establish and implement an adequate AML program. The four commonly recognized touch stones for such programs include: (1) a system of internal controls commensurate with the risks, (2) independent testing of the controls, (3) responsible individual(s) for day-to-day compliance, and (4) adequate training for personnel. Merchants was judged to

have failed all four. Noteworthy among the findings was that the Bank's insiders interfered with the BSA staff's attempts to investigate compliance and to report non-compliance, often with threats of possible dismissal or career retaliation.

Further, FinCEN focused on the fact that many of Merchants' MSBs were high-risk customers. For example, one of Merchants' check-cashing customers was physically located along the Mexican border, which FinCEN recognized as increasing the likelihood that its source of funds came from Mexico. However, Merchants did not sufficiently monitor or analyze that customer's account activity, nor did it conduct any heightened due diligence to identify the source of funds for the customer's check-cashing business.

Merchants failed to designate a BSA officer to ensure day-to-day compliance with the BSA. Rather, Merchants assigned various individuals with little knowledge or adequate training of the BSA. Most alarming was that two of the individuals primarily tasked with ensuring compliance with the BSA were Merchants' executives in charge of bringing MSB business to the bank, thereby creating a recognizable conflict of interest.

The second primary violation found by FinCEN was Merchants failure to conduct required due diligence on its foreign correspondent accounts. For example, Merchants had four banking customers located in many high-risk jurisdictions, but failed to identify and report these as foreign correspondent customers. This failure resulted in Merchants not implementing the required customer due diligence program. During a three-month period, these four customers sent and received a total of \$192 million in wire transfers. It appears that Merchants simply failed to report any of the wired transactions as suspicious to FinCEN.

Lastly, FinCEN found that Merchants failed to comply with its Suspicious Activity Reporting ("SAR") obligations. According to FinCEN, a transaction is suspicious if it: 1) involves funds derived from illegal activities, 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 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. FinCEN reported that from 2012 to 2016, Merchants failed to adequately monitor billions of dollars of transactions for suspicious activity which led to Merchants failing to file or timely file on hundreds of millions of dollars of suspicious activity.

On a matter of special interest for lawyers practicing in the electronic banking space is FinCEN's discussion of Merchants' remote deposit capture ("RDC") practices. In the rush to join the parade of the latest and greatest customer-friendly technologies, bankers must not forget that RDCs, like all technology products, have risks which the regulators are demanding be adequately investigated, understood and planned for through implemented policies. FinCEN determined that Merchants failed to implement adequate controls for the RDC services offered to its far flung high-risk MSBs. Those failures included the lack of basic banking infrastructure necessary to understand the true scope of its RDC offering and usage, being unprepared to detect suspicious RDCs, and not having a tailored customer risk-rating plan for all customers using the service.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.