On the WLF Legal Pulse

Timely commentary from WLF's blog December 19, 2022

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

Compliance Lessons from Danske Bank's $2B Fraud Guilty Plea

by Gregory A. Brower

On December 13, Denmark-based multinational banking and financial services company, Danske Bank A/S, pleaded guilty in U.S. District Court to one count of conspiracy to commit bank fraud and agreed to forfeit more than $2 billion* to resolve a long-running investigation into its relationships with certain U.S. banks. Dansk Bank admitted to defrauding these banks by misrepresenting the details of one of its business unit's anti-money laundering ("AML") compliance program. In announcing the resolution, Deputy Attorney General Lisa Monaco emphasized that DOJ "expects companies to invest in robust compliance programs—including at newly acquired or far-flung subsidiaries—and to step up and own up to misconduct when it occurs." The detailed statement of facts that accompanied the plea agreement suggests several potential lessons for corporate compliance efforts.

This criminal resolution follows Danske Bank's disclosure in 2018 that an internal investigation revealed significant AML compliance lapses in its Estonian banking unit. Specifically, the statement of facts which accompanied the plea agreement acknowledged that the Estonian operations included customers from Russia and other former Soviet bloc countries who routinely transferred larger amounts of money through the bank with little or no scrutiny for potential money laundering. As is so often the case in the Foreign Corrupt Practices Act ("FCPA") context, the problem here seems to have been related, at least in part, to Danske Bank's 2007 acquisition of a smaller Finland-based bank that had a significant and very lucrative business in Estonia. Following the acquisition, however, the new Estonian operations were never fully integrated into Danske Bank's corporate systems apparently creating some compliance gaps.

This DOJ investigation was different from others focused on the sufficiency of financial institutions' AML programs in light of U.S. Bank Secrecy Act ("BSA") requirements. Here, as noted above, DOJ charged Danske Bank with conspiracy to commit bank fraud, not a violation of the BSA, and the reason seems to be two-fold. First, a foreign financial institution not operating in the U.S. would not be subject to the BSA and thus DOJ would not have jurisdiction. Second, the evidence in this case revealed more than an adequate AML compliance program; there was also evidence that the defendant bank actually conspired to commit fraud on its U.S. bank partners in violation of 18 USC § 1349 by mischaracterizing its AML compliance program within is Estonian operations.

* DOJ agreed to credit nearly $850 million in payments the company has made or will make to resolve related investigations by other U.S. and foreign agencies. (See May 19, 2018 memorandum from Deputy Attorney General Rod J. Rosenstein entitled "Policy on Coordination of Corporate Resolution Penalties.")

Gregory A. Brower is Chief Global Compliance Officer for Wynn Resorts. He also serves on WLF Legal Policy Advisory Board and is a former U.S. Attorney.

Despite the prosecution's focus on bank fraud instead of the BSA itself, the plea agreement's detailed statement of facts is nevertheless full of potential lessons for U.S. financial institutions and their AML compliance efforts. These include, among others, the following:

(1) *Ensure Transparency Through Accuracy*. The hallmark of any effective AML compliance program is transparency. After all, the whole point of the BSA is accurate recording and timely reporting of certain types of cash transactions and suspicious activity by the financial institution's customers. Here, Danske Bank admitted that its employees conspired with customers to shield the true nature of their transactions, including assisting customers with the creation of shell companies to disguise these transactions. Such practices are more than passive failures to maintain an adequate AML program and really amount to affirmative actions that are fundamentally at odds with the purpose of such a program and are therefore likely to draw enforcement action. To be effective, an AML program, above all else, must ensure that transactions are booked accurately.

(2) *Know Your Customer*. Danske Bank also admitted that its Estonian business unit's practices and procedures allowed customers to open accounts and conduct transactions without appropriate due diligence. Like accurate recording and timely reporting, "know your customer" or "KYC" has become a required part of any effective AML compliance program and all financial institutions must know that their customers genuinely are who they claim to be. In order to be effective, a KYC program should include accurate customer identification on the front end, followed by further customer due diligence to establish a specific risk profile, and finally enhanced due diligence to obtain greater details on certain high-risk customers. An AML program that does not include accurate KYC simply cannot be effective and is subject to scrutiny for noncompliance with the applicable AML laws and regulations.

(3) *Be Honest About Your Business Model and Compliance Program*. As noted above, Danske Bank was charged with and pled guilty to bank fraud, demonstrating that even a bank can commit bank fraud. Here, Danske Bank's U.S. bank partners, so-called "correspondent banks," required it to respond to periodic inquiries regarding particular transactions and customers and about its AML compliance program generally. This is a common way for financial institutions to assess the risk of doing business with other financial institutions. Despite knowing that the accuracy of such information was material to the U.S. banks' willingness to do business with them, Danske Bank misrepresented certain material facts, including the state of its AML compliance program in Estonia, thus causing the U.S. banks to facilitate billions in transactions without full awareness of the potential money laundering risk that accompanied those transactions. This case shows that any company, whether a financial institution or an ordinary customer, that intentionally and materially mischaracterizes its business model to a U.S. bank, including its AML program, is potentially committing bank fraud in the eyes of DOJ.

(4) *Adequately Invest in Technology*. When Danske Bank acquired the smaller Finland-based bank and its Estonia business in 2007, it initially undertook to migrate the new operations into its central technology system because it recognized that certain AML risks could arise by allowing the new Estonian operations to remain outside of its central IT platform. However, Danske Bank abandoned that migration plan because its senior leadership judged the plan too expensive, and the Estonian branches were allowed to continue to operate outside the larger IT system. This did, in fact, create AML compliance issues which ultimately led to a criminal investigation. Whether it's the integration of a newly acquired business or an upgrade to a newer, more capable system, technology that enhances compliance, especially AML compliance, must be a priority for any company. Failing to properly prioritize compliance-technology investments inevitably leads to larger costs, including additional employees to do the work less efficiently, fines and penalties resulting from enforcement

actions that could have been avoided by better compliance technology, and the reputational harm that can result from such enforcement actions.

(5) *Timely Address Deficiencies*. The Danske Bank statement of facts revealed that in 2013, an insider raised concerns about AML deficiencies within the company's Estonian operations and, in response, the company conducted targeted audits that confirmed certain problems. That discovery led to a more comprehensive review which validated the initial concerns. Unfortunately, Danske Bank's response to these findings was found to be "insufficient and delayed" and did not result in any disclosures to regulators despite legal counsel's recommendation that such disclosures be made. Later, company executives rejected a proposal to conduct a further independent investigation because of concerns that it would lead to "additional drama." Ignoring whistleblower concerns or, worse yet, determining them to be credible but then doing nothing to address them can lead to disastrous results. No compliance program is perfect. Credible information about a potential problem must be addressed in a timely and effective manner with adequate and accurate documentation, especially if, for whatever reason, remedial action is not taken.

DOJ has recently made it clear that it expects every company to make compliance a priority and has encouraged a focus on prevention. The Danske Bank resolution is yet another example of how underfunded, ineffective compliance programs can undermine prevention efforts and lead to significant enforcement actions, proving once again that an ounce of prevention truly is worth a pound (or 2 billion pounds) of cure.