THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 39 No. 4 April 2023

PRE-PUBLICATION ISSUE

UNITED STATES V. DANSKE BANK: NEW THEORY OF LIABILITY FOR VIOLATION OF U.S. AML STANDARDS

This Article discusses the recent plea agreement between the United States and Danske Bank. It argues that the Department of Justice has advanced a new and evolving theory of liability for foreign banks that access the U.S. financial system through correspondent banking relationships. This theory of liability has expansive extraterritorial reach because such foreign banks provide extensive representations about their anti-money laundering and sanctions compliance programs at account opening and on an ongoing basis. If those representations are deemed false, they could be the basis of criminal liability if supported by other elements of bank fraud — even if the foreign bank has no subsidiary, branch, or other presence in the United States.

By Michael Dawson and Michael Leotta *

Late last year, Danske Bank A/S pleaded guilty to one count of conspiracy to commit bank fraud in violation of 18 U.S.C. Section 1349 and agreed to a money judgment of $2,059,979,050.[1] The plea agreement is notable not only because it is the largest financial penalty imposed in a matter whose root lies in violation of anti-money laundering ("AML") standards, but also because it entails a new theory of liability with broad implications for the extra-territorial application of U.S. AML standards. The matter also reflects the evolving enforcement policy of the Department of Justice in corporate criminal matters, particularly a policy preference for guilty pleas over deferred prosecution agreements; expectations for securing credit for cooperation; and requirements for compliance commitments, including evaluating the compliance performance of executives and rendering executives with a "failing score" ineligible for bonuses.

THE FACTS

Danske Bank is headquartered in Copenhagen and is the largest bank in Denmark. It has had both a retail and a commercial business. As of 2022, it had approximately $600 billion in assets.[2] Its activities have been concentrated in the Nordics, with some efforts to expand into additional markets, including the United Kingdom, Ireland, and, as we shall see, the Baltics. Notably, and unlike many other foreign banking organizations of similar size and prominence, Danske

[1] Consent Preliminary Order of Forfeiture / Money Judgment, *United States v. Danske Bank A/S*, 22 Cr. 679 (NRB) (S.D.N.Y. Dec. 12, 2022) (The plea agreement was signed on December 12 and filed on December 13).

[2] "Danske Bank," Forbes (profile accessed Jan. 30, 2023) *available at*: https://www.forbes.com/companies/danske-bank/?sh=3d1de42b4242.

* *MICHAEL DAWSON and MICHAEL LEOTTA are partners at WilmerHale's Washington, DC office. Their e-mail addresses are michael.dawson@wilmerhale.com and michael.leotta@wilmerhale.com.*

RSCR Publications LLC Published 12 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $650 per year in U.S., Canada, and Mexico; $695 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. Copyright © 2023 by RSCR Publications LLC. ISSN: 1051-1741. All rights reserved. Reproduction in whole or in part prohibited except by permission. For permission, contact Copyright Clearance Center at www.copyright.com. *The Review of Banking & Financial Services* does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions, or for the results obtained from the use of such information.

Bank does not — and did not during the period at issue — have a banking subsidiary or branch in the United States.

The facts that gave rise to the plea agreement have their origin in 2007, when Danske Bank acquired Finland-based Sampo Bank, including Sampo Bank's subsidiary in Estonia. As stated in the Information, "[a] significant portion of Sampo Bank's Estonia business was providing banking services to non-resident customers, that is, companies and individuals residing outside Estonia, including in Russia," a business that the Information termed the "non-resident portfolio" ("NRP").

Many of the customers in the NRP conducted transactions in U.S. dollars. This, in turn, required Danske Bank to route the transactions through banks in the United States using what are known as "correspondent banking relationships." As described in the Information, Danske Bank "knew that the NRP was high risk because, among other reasons, its customers resided in high-risk jurisdictions, frequently used shell companies to shield the identity of their ultimate beneficial owner or the sender or recipient of transactions, and engaged in suspicious transactions through U.S. banks." The Information identifies three of Danske Bank's U.S. banks — "U.S. BANK 1," "U.S. BANK 2," and "U.S. BANK 3" — as having provided correspondent banking relationships to Danske Bank.

Eventually, Danske Bank "determined that Danske Bank Estonia processed through the U.S. Banks billions of dollars in transactions associated with money laundering and other criminal schemes, including Russian criminal schemes." Media stories assert that Danske Bank Estonia processed as much as €280 billion in such transactions, much of which was allegedly the proceeds of crimes, such as tax evasion in foreign countries, principally Russia.

The Information states that Danske Bank Estonia "attracted NRP customers by ensuring that they could transfer large amounts of money through Danske Bank Estonia with very little, if any, oversight or scrutiny." It further states that employees "conspired with their customers to shield the true nature of their transactions, including by assisting customers to conceal beneficial owners by establishing accounts for known shell companies and sometimes creating shell companies for customers in exchange for a 'consulting fee.'" But the Information sheds little light on important aspects of the money laundering itself. Who laundered the funds? What financial institutions did the funds come from before they were deposited in Danske Bank? Where did the laundered funds go once they left Danske Bank? Have any of the laundered funds been seized? The Information is silent on these questions.

What the Information does elaborate on are Danske Bank's misrepresentations to its banks in the United States — indeed, it is those misrepresentations, not money laundering by Danske Bank employees or a willful failure to maintain anti-money laundering controls, that forms the basis of the plea agreement. Specifically, the Information focuses on information that Danske Bank provided U.S. BANK 1 and 2 at account opening and on an ongoing basis regarding its AML compliance program and controls. For example, in response to concerns raised by U.S. BANK 1 about the NRP, Danske Bank Estonia provided "false" assurances that it had taken "mitigating steps, including automatic sanctions and AML monitoring, client visits, and a prohibition on third-party agents." Other false statements included, among others:

- Falsely characterizing the extent of due diligence on NRP customers to representatives of U.S. BANK 1 during a standard compliance visit;

- Misrepresenting that "Danske [Bank Estonia] does not advise clients to restructure their business after enquiries from [U.S. Bank 1]";

- After learning that it was losing the ability to conduct correspondent banking transactions with U.S. BANK 1, misrepresenting "the reason it was seeking a new account" to U.S. BANK 3;

- Representing that "Danske Bank Estonia had 'approved AML policies and procedures in place that require[d] the identification and verification of the Beneficial Ownership of . . . corporate customers'" when "the actual procedures . . . followed were inconsistent with the written policies"; and

- Falsely answering “yes” to three questions on U.S. BANK 3’s Financial Institution Anti-Money Laundering Questionnaire.

The government alleges that instead of answering the U.S. banks’ due-diligence and money-laundering-investigation questions truthfully, Danske Bank intentionally lied in order to maintain or open correspondent banking accounts through which it processed $160 billion for its non-resident customers.

THE EXTRATERRITORIAL REACH OF THE THEORY

It is important to understand just how expansive this new theory of liability for foreign banks is. Virtually every foreign bank of significant size and prominence in their local economies will have clients that wish to transact in dollars. For example, personal customers may wish to pay tuition for a child studying at a U.S. university. As another example, corporate customers that export goods may need to receive payments in dollars from importers in the United States and other countries. As a result, foreign banks need some way of processing dollar-denominated transactions on behalf of their customers. Some foreign banks may do this through a branch or subsidiary in the United States, but many foreign banks — particularly if they are not large enough to support a business case for acquiring a subsidiary or opening a branch — will be able to do so only by establishing and maintaining a correspondent banking relationship with a U.S. clearing bank.

But opening and maintaining a correspondent banking account is by no means a pro forma exercise. Congress and the banking regulators have long regarded correspondent banking as high risk. In March 2001, the Permanent Subcommittee on Investigations of the U.S. Senate issued a report of extensive hearings and investigations entitled, “Role of U.S. Correspondent Banking in International Money Laundering.” The Report included a report by the Minority Staff that termed correspondent banking a “Gateway to Money Laundering.” The Minority Staff’s Report found that “U.S. banks, through the correspondent accounts they provide to foreign banks, have become conduits for dirty money flowing into the American financial system and have, as a result, facilitated illicit enterprises, including drug trafficking and financial frauds. Correspondent accounts in U.S. banks give the owners and clients of poorly regulated, poorly managed, sometimes corrupt, foreign banks with weak or no anti-money laundering controls direct access to the U.S. financial system and the freedom to move money within the United States and around the world.”

Six months later, following the terrorist attacks of September 11, 2001, Congress began crafting a package of measures that would come to be known as the USA PATRIOT ACT. The Act included a number of amendments to the anti-money laundering provisions of the Bank Secrecy Act, including a requirement to conduct special due diligence on foreign correspondent account relationships.[3]

As a result of Section 312 and its implementing regulations, U.S. banks seek information from foreign banks seeking to open or maintain correspondent accounts with them, including information on the foreign banks’ AML and sanctions compliance programs. The information sought is usually detailed and extensive, as it was in the Danske Bank case. The Wolfsberg Group publishes and updates a Correspondent Banking Due Diligence Questionnaire (“CBDDQ”) and associated guidance,[4] which runs to over 100 questions, many of which are multi-part. The CBDDQ includes questions ranging from basic factual information about the foreign bank, such as its legal name, address, and date of establishment, to more substantive information, such as whether the foreign bank has a “programme that sets minimum AML, CTF and Sanctions standards” with respect to 15 enumerated components. Examples of other questions include:

- Does the foreign bank “have risk-based policies, procedures, and monitoring processes for the identification and reporting of suspicious activity?”
- Does the foreign bank “adhere to the Wolfsberg Group Payment Transparency Standards?”
- Does the foreign bank “have policies, procedures, or other controls reasonably designed to prohibit and/or detect actions taken to evade applicable sanctions prohibitions?”

In short, numerous foreign banks must have a correspondent banking relationship with U.S. banks if they are to meet the needs of their customers. To obtain

[3] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, PUBLIC LAW 107–56 — OCT. 26, 2001, Section 312, codified at 18 U.S.C. Section 5318(i).

[4] The Wolfsberg Group “is an association of 13 global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.” https://www.wolfsberg-principles.com/about/mission.

and maintain the relationships, the foreign banks must provide extensive information about their compliance programs. Following the plea agreement in *U.S. v. Danske Bank*, it is clear that foreign banks risk significant criminal liability in the United States if they intentionally submit false information in response to the U.S. banks' AML inquiries.

This case is not an aberration but is a part of an evolving effort by DOJ to use the U.S. criminal code to go after those who evade U.S. banks' own compliance efforts. In March 2021, one of the same federal prosecutors who brought the case against Danske Bank brought an analogous conspiracy to commit bank fraud case in the Southern District of New York. In *U.S. v. Weigand* (SDNY 1:20-cr-00188), the U.S. Attorney's Office convicted two businessmen of bank fraud conspiracy for using false merchant category codes to trick banks into processing more than $150 million of credit card transactions on behalf of San Francisco-based Eaze, a cannabis-selling app nicknamed "the Uber of pot." The cannabis purchases themselves were lawful under California state law, and it was uncontested that the credit-card holders wanted to use their credit cards to purchase the cannabis —no customers were alleged to be harmed and no funds stolen. Nor did the banks lose money. To the contrary, the defense argued that the allegedly defrauded banks profited by receiving fees from processing the payments. Nevertheless, the government brought a bank-fraud-conspiracy charge because the banks would not have processed these credit-card transactions at all if they had known they were for cannabis purchases. The evidence at trial showed that the banks and credit-card companies used multiple, proactive means to try to detect cannabis-related transactions and would remove cannabis merchants from their platforms if identified, even where such sales were lawful under state law. By using false merchant category codes, the defendants concealed the nature of the payments from the banks, thereby allowing the customers to purchase cannabis with their credit cards without triggering the banks' compliance controls. The defendants were convicted and sentenced to 30 and 15 months' imprisonment, in addition to forfeiture and fines.

As the *Danske Bank* and *Weigand* prosecutions show, false statements that are intended to deceive a U.S. bank — and thereby evade its compliance efforts — may be prosecuted as bank fraud even where the bank did not lose any money. Because banks are gatekeepers to the U.S. financial system, the U.S. AML regime relies upon banks' own compliance programs to detect and inform the government about potential wrongdoing, and U.S. law enforcement will police any efforts to evade those controls.

To obtain and maintain the relationships, the foreign banks must provide extensive information about their compliance programs. Following the plea agreement in *U.S. v. Danske Bank*, it is clear that this information could expose foreign banks to criminal liability in the United States if the information subsequently is found to be false.

INCREASED FOCUS ON EXECUTIVE COMPENSATION AND COMPLIANCE

In addition to the expansive theory of liability, the plea agreement sheds light on the Department of Justice's evolving expectations for compliance commitments. The plea agreement includes a number of compliance commitments with respect to the AML compliance program and "compliance programs related to fraudulent conduct by employees, employee ethics, and whistleblowers." Many of these are commitments that have become commonplace in corporate plea agreements, including:

- Tone at the top — ensuring "that its directors and senior management provide strong, explicit, and visible support and commitment to its Compliance Programs and demonstrate rigorous adherence by example";
- Policies and procedures — maintaining, or where necessary, developing and promulgating "clearly articulated and visible corporate policies" that address AML, bank fraud, and the observance of ethics, including policies that address 15 specific items that go beyond elements typically seen in an AML policy, including:
  - — Conflicts of interest;
  - — Payments from outside sources;
  - — Provision of information to U.S. correspondent banks; and
  - — Whistleblowing;
- Periodic risk-based reviews — enhancing its compliance programs "based on regular, periodic risk assessments . . . taking into account, but not limited to, its global operations, geographical organization, industrial sectors of operations, various business lines and products, potential and

current customers, and U.S. financial institution relationships";

- Training and Guidance — maintaining or implementing "mechanisms designed to ensure that the Compliance Programs are effectively communicated to all directors, officers, employees, and, where necessary and appropriate, agents and business partners"; and

- Monitoring and Testing — conducting "periodic reviews and testing of the Compliance Programs."

The Compliance Commitments, like the compliance commitments in other major corporate plea agreements and deferred prosecution agreements, also include a commitment regarding enforcement and discipline of the Compliance Programs. But these commitments go farther. They require Danske Bank to "implement evaluation criteria related to compliance in its executive review and bonus system so that each Bank executive is evaluated on what the executive has done to ensure that the executive's business or department is in compliance with the Compliance Programs and applicable laws and regulations." The Commitments provide that "[a] failing score in compliance will make the executive ineligible for any bonus that year." In these respects, the commitments go farther than other recent agreements, which included only general commitments to enforcement and discipline, as well as to "incentivize compliance." Indeed, the Department of Justice has since announced that it is updating its policies regarding executive compensation and clawbacks in general.

CONCLUSION

U.S. v. Danske Bank is important not just because of its large penalty. It is important because it puts virtually every non-U.S. bank of substance on notice that if it wishes to transact in dollars through a correspondent account with a U.S. bank, it will have to develop and maintain AML, sanctions, and other compliance programs that will meet U.S. banks' standards and accurately communicate the status of those programs to U.S. banks. This should further improve the state of AML, sanctions, and other compliance standards in banks around the world. ■