Press Release

November 4, 2015

Contact: Matt Anderson, 212-709-1691

NYDFS ANNOUNCES DEUTSCHE BANK TO PAY $258 MILLION, INSTALL INDEPENDENT MONITOR, TERMINATE EMPLOYEES FOR TRANSACTIONS ON BEHALF OF IRAN, SYRIA, SUDAN, OTHER SANCTIONED ENTITIES

Deutsche Bank Created "OFAC-Safe" Payment Processing Schemes to Evade U.S. Treasury Office of Foreign Asset Control (OFAC) Sanctions

Deutsche Bank Employee Email: "Let's not revert to the client in writing due to the reputational risk involved if the e-mail goes to wrong places. Someone should call [the client] and tell them orally and ensure that the conversation is not taped. . . . Let's also keep this e-mail strictly on a 'need-know' basis, no need to spread the news…what we do under OFAC scenarios"

Anthony J. Albanese, Acting Superintendent of Financial Services, today announced that Deutsche Bank will pay $258 million and install an independent monitor for New York Banking Law violations in connection with transactions on behalf of countries and entities subject to U.S. sanctions, including Iran, Libya, Syria, Burma, and Sudan. Additionally, while several of the employees who were centrally involved in this misconduct no longer work at the Bank, Deutsche Bank will take action to terminate an additional six employees involved in the scheme who currently remain employed by the Bank; and ban three other employees from any duties involving the firm's U.S. operations. The overall $258 million penalty Deutsche Bank will pay includes $200 million to the New York State Department of Financial Services (NYDFS) and $58 million to the Federal Reserve.

Acting Superintendent Albanese said: "We are committed to investigating and pursuing sanctions violations and money laundering at financial institutions. We are pleased that Deutsche Bank worked with us to resolve this matter and take action against individual employees who engaged in misconduct. To truly deter future wrongdoing, it is important to focus not just on corporate accountability, but also individual accountability."

Wire Stripping and Non-Transparent Cover Payments to Disguise Transactions

From at least 1999 through 2006, Deutsche Bank used non-transparent methods and practices to conduct more than 27,200 U.S. dollar clearing transactions valued at over $10.86 billion on behalf of Iranian, Libyan, Syrian, Burmese, and Sudanese financial institutions and other entities subject to U.S. economic sanctions, including entities on the Specially Designated Nationals ("SDN") List of the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC").

Starting at least in 1999, Bank employees recognized that U.S. sanctions rules, which applied at that time or over the course of subsequent years to Iranian, Syrian, Libyan, Burmese, or Sudanese customers or to customers who were listed on OFAC's SDN list, would pose problems for U.S. dollar payments sent to or cleared through the U.S., including clearing done through Deutsche Bank New York. Payments involving sanctioned entities were subject to additional scrutiny and might be delayed, rejected, or frozen in the United States. In order to facilitate what it saw as "lucrative" U.S. dollar business for sanctioned customers, Bank employees developed and employed several processes to handle dollar payments in non-transparent ways that circumvented the controls designed to detect potentially-problematic

payments.

One method was wire stripping, or alteration of the information included on the payment message. Bank staff in overseas offices handling Message Type 103 serial payment messages, or MT103s, removed information indicating a connection to a sanctioned entity before the payment was passed along to the correspondent bank in the U.S. With any potentially-problematic information removed (or, as was done in some cases, replaced with innocuous information, such as showing the bank itself as the originator), the payment message did not raise red flags in any filtering systems or trigger any additional scrutiny or blocking that otherwise would have occurred if the true details were included.

A second method was the use of non-transparent cover payments. The cover payment method involved splitting an incoming MT103 message into two message streams: an MT103, which included all details, sent directly to the beneficiary's bank, and a second message, an MT202, which did not include details about the underlying parties to the transaction, sent to Deutsche Bank New York or another correspondent clearing bank in the U.S. In this way, no details that would have suggested a sanctions connection and triggered additional delay, blocking, or freezing of the transactions were included in the payment message sent to the U.S. bank.

Bank employees recognized that these handling processes were necessary in order to evade the sanctions-related protections and controls of Deutsche Bank New York and other correspondents. For example, a relationship manager who handled significant business for Iranian, Libyan, and Syrian customers explained the need for special measures as follows, in a 2003 email to colleagues: The Bank employs "specific precautionary measures that require a great deal of expertise" because "[i]f we make a mistake, the amounts to be paid could be frozen in the USA and/or DB's business interests in the USA could be damaged." Or as the Assistant Vice President who oversaw payments processing explained to a colleague who inquired about Iranian payments, **the Bank needed to employ "the tricks and cunning of MT103 and MT202" because of the U.S. sanctions restrictions otherwise applicable to sanctions-related payments**.

The special processing that the Bank used to handle sanctioned payments was anything but business as usual; it required manual intervention to identify and process the payments that needed "repair" so as to avoid triggering any sanctions-related suspicions in the U.S. Indeed, on occasion, customers whose payments received this special processing questioned the extra fees the bank was charging for the manual processing. They were told that this is what was necessary in order to circumvent the U.S.-based sanctions controls.

Bank relationship managers and other employees worked with the Bank's sanctioned customers in the process of concealing the details about their payments from U.S. correspondents.

During site visits, in emails, and during phone calls, clients were instructed to include special notes or code words in their payment messages that would trigger special handling by the bank before the payment was sent to the United States. Sanctioned customers were told "it is essential for you to continue to include [the note] 'Do not mention our bank's name…' in MT103 payments that may involve the USA. [That note] ensures that the payments are reviewed prior to sending. Otherwise it is possible that the [payment] instruction would be sent immediately to the USA with your full details. . . . [This process] is a direct result of the US sanctions." Customers, in turn, included notes in free-text fields of SWIFT messages such as "Please do not mention our bank's name or SWIFT code in any msg sent via USA," **"PLS DON'T MENTION THE NAME OF BANK SADERAT IRAN OR IRAN IN USA," or "THE NAME BANK MELLI OR MARKAZI SHOULD NOT BE MENTIONED . . . IMPORTANT: NO IRANIAN NAMES TO BE MENTIONED WHEN MAKING PAYMENT TO NEW YORK."**

But the Bank did not rely on the customer notes and code words alone; the Bank's payments processing staff were instructed to be on the lookout for any payment involving a sanctioned entity and ensure that no name or other information that might arouse sanctions-related suspicions was sent to the U.S. correspondents, even if the customer failed to include a special note to that effect.

In fact, the Bank's **"OFAC-safe"** handling processes and its experience in handling sanctions-related payments were selling points when soliciting new business from customers subject to U.S. sanctions. On one occasion, a relationship manager visiting a Syrian bank during a time when the U.S. was considering instituting certain Syrian sanctions pitched Deutsche Bank's "OFAC-safe vehicles," and when the client mentioned possibly splitting its business among several Asia-based banks, the relationship manager "highlighted that the Asian banks in general are not very familiar with OFAC procedures [and] [a]sked them to consider who their friends will be in the longer run, DB or Asian banks." **In another instance, after Deutsche Bank staff responded to a client inquiry about handling U.S. dollar payments relating to Iran and Syria with a favorable "OFAC safe" solution, the Bank relationship manager reported that the client was so pleased that it "used the opportunity to enquire whether we can also do USD payments into Burma/Myanmar."**

The practice of non-transparent payment processing was not isolated or limited to a specific relationship manager or small group of staff. Rather, Bank employees in many overseas offices, in different business divisions, and with various levels of seniority were actively involved or knew about it. In addition, some evidence indicates that at least

one member of the Bank's Management Board was kept apprised about and approved of the Bank's business dealings with customers subject to U.S. sanctions.

Certain non-U.S. employees, especially those who managed relationships with a high number of Iranian, Libyan, or Syrian clients or who regularly processed U.S. dollar payments for sanctioned customers, were considered experts in the bank's "OFAC-safe" handling procedures. They regularly educated colleagues in other branches or in other divisions outside the U.S. about handling U.S. dollar payments.

Moreover, the Bank disseminated formal and informal written instructions emphasizing the need for utmost care to ensure that no sanctions-related information was included in U.S.-bound payment messages and setting out the various methods to use when processing sanctions-related payments. For example, Deutsche Bank staff told investigators that during the earlier part of the relevant time period, an internal customer database included notes for certain sanctioned customers indicating that their name must not be referenced in payment messages sent to the U.S.

Later, Bank payments processing employees prepared a training manual for newly-hired payments staff in an overseas office. The manual included a section titled "US Embargo Payments" that explained how to handle payments with a sanctions connection. An early draft included a warning, in bolded text: "Special attention has to be given to orders in which countries/institutes with embargos are involved. Banks under embargo of the US (e.g., Iranian banks) must not be displayed in any order to [Deutsche Bank New York] or any other bank with American origin as the danger exists that the amount will be frozen in the USA."

A revised version of the payments manual admonished that payments from Iran and Syria "have to be treated with caution as [ ] the payment gets released from the queue; there is a probability that the funds will be frozen by the Federal Reserve thereby causing financial and reputation loss for the Bank." A later version of the manual noted that the payment message might include key words such as "Embargo" or "Do not pay via US," but it also cautioned employees that code words might not necessarily be present. In any event, non-U.S. employees were instructed that information linking a customer to a U.S. sanctions program must not be displayed in any message sent to Deutsche Bank New York or any other American bank. The preference, they were told, was to send two messages (that is, to use the cover payment method), but if that was not possible, they must reformat the message so that it gets routed for additional repair and reformatting "in such a way that the Embargo names are not visible to the receiving US banks." The manual included computer screenshots illustrating how these problematic messages might appear and how to handle them.

Moreover, less formal instructions were disseminated to certain staff via email throughout the relevant time period. In one email chain regarding possible recruitment of a new customer with Libyan connections, Bank staff were cautioned to "please be careful in regard to the US, since it does violate OFAC," and were told, "please do not mention OFAC names in the subject line of e-mails!" In another instance, when certain U.S. regulations against a Syrian bank were imposed in 2004, relevant employees were told: "Let us be very careful while effecting USD denominated transaction[s] with Syria. In case we have to effect any USD denominated remittance to Syria, please ensure that name of Syria should not appear in the message."

At the same time, Bank staff took care to avoid publicizing details about their non-transparent payments handling, both within and outside the bank. Employees recognized the legal and reputational concerns and acted to keep the payment handling methods – and indeed the fact of the bank's business dealings with sanctioned entities in general – **on a need-to-know basis.**

For example, one non-U.S. relationship manager who asked for advice about U.S. dollar processing was told, "Please be informed that any info on OFAC-safe business patterns (THAT DB does it and HOW DB does it) is strictly confidential information. Compliance does not want us to distribute such info to third parties, and forbids us explicitly to do so in any written or electronic form." In another email, a senior compliance executive with oversight of this area told a non-U.S. relationship manager who was asking about the possibility of doing business with a Syrian customer that Compliance "agreed to do business on a low key level without public announcements etc." Later, when that relationship manager was offering advice to another non-U.S. colleague about assisting a client who needed to make and receive U.S. dollar payments with Iranian and Syrian connections, he cautioned his colleague: **"As usual, let's not revert to the client in writing due to the reputational risk involved if the e-mail goes to wrong places. Someone should call [the client] and tell them orally and ensure that the conversation is not taped. . . . Let's also keep this e-mail strictly on a 'need-know' basis, no need to spread the news in [Deutsche Bank's Asian offices about] what we do under OFAC scenarios."**

Around the same time, that same relationship manager told another non-U.S. colleague: "Please note that while DB is prepared to do business with Syria, we obviously have sizeable business interests in the US, too, which DB wants to protect. So any Syrian transaction should be treated STRICTLY confidential and should involve any colleagues on a 'Must-Know' basis only! . . . [W]e do not want to create any publicity or other 'noise' in the markets or media."

In addition, while one of the main purposes of the nontransparent practices was to keep the Bank's U.S. staff in the

dark about the sanctions connections of the payments they were processing, Deutsche Bank New York staff occasionally raised objections to the Bank's business relationship with U.S.-sanctioned parties based on U.S. law. Their European colleagues, however, did nothing to stop the practice but instead redoubled their efforts to hide the details from their American colleagues. For example, a relationship manager who did significant business with Iranian and Syrian customers complained to his boss that colleagues in the Middle East "participated in a major conference call with senior management of [Deutsche Bank New York] and provided an overview of DB's account activities with Syria outside the U.S. Senior management of [Deutsche Bank New York] complained strongly to DB Frankfurt that they see this as a breach of law." **The relationship manager viewed this incident not as a prompt to re-examine the bank's Syrian business, however, but rather as indicating a need to better train the non-U.S. staff who handle the "very lucrative" Syrian and Iranian business to ensure such disclosures do not occur in the future.**

Termination of Deutsche Bank Employees under DFS Order

While several of the Bank employees who were centrally involved in the improper conduct discussed in this Consent Order no longer work at the Bank, six such employees do remain employed by the Bank. DFS has ordered the Bank to terminate those six employees: a managing director in Global Transactions Banking; a managing director in Operations; a director in Operations; a director in Corporate Banking and Securities; a vice president in Global Transactions Banking; and a vice president/relationship-manager. Additionally, three other Deutsche Bank employees will be banned from holding any duties, responsibilities, or activities involving compliance, U.S. dollar payments, or any matter relating to U.S. operations.

Acting Superintendent Albanese thanked the Federal Reserve for their work and cooperation in this matter.

To view a copy of the DFS consent order regarding Deutsche Bank, please visit, **link**.

###