U.S. Department of Justice

United States Attorney
Southern District of New York

Criminal Division
Money Laundering and Asset Recovery Section

The Silvio J. Mollo Building
One Saint Andrew's Plaza 950
New York, New York 10007

Bond Building
1400 New York Ave, NW
Washington, D.C. 20005

December 12, 2022

Katherine J. Stoller, Esq.
Shearman & Sterling LLP
599 Lexington Avenue
New York, New York 10022

22 CRIM 679

Samuel W. Seymour, Esq.
Sharon Cohen Levin, Esq.
Sullivan & Cromwell LLP
125 Broad Street
New York, New York 10004

Re: *United States v. Danske Bank A/S*

PLEA AGREEMENT

Pursuant to Rule 11(c)(1)(C) of the Federal Rules of Criminal Procedure, the United States of America, by and through the Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section ("MLARS"), and the United States Attorney's Office for the Southern District of New York ("the USAO-SDNY") (collectively the "Offices"), and the Defendant, DANSKE BANK A/S (the "Defendant" or the "Bank"), by and through its undersigned attorneys, and through its authorized representative, pursuant to authority granted by the Defendant's Board of Directors, hereby submit and enter into this plea agreement (the "Agreement"). The terms and conditions of this Agreement are as follows:

Term of the Defendant's Obligations Under the Agreement

1. Except as otherwise provided in Paragraph 12 below in connection with the Defendant's cooperation obligations, the Defendant's obligations under the Agreement shall last and be effective for a period beginning on the date on which the Information is filed and ending three years from the date on which the Information is filed (the "Term"). The Defendant agrees, however, that in the event the Offices determine, in their sole discretion, that the Defendant has knowingly violated any provision of this Agreement or failed to completely perform or fulfill each of the Defendant's obligations under this Agreement, the Offices, in their sole discretion, may impose an extension or extensions of the Term for up to a total additional time period of one year, without prejudice to the Offices' right to proceed as provided in Paragraphs 26-28 below. Any extension of the Term extends all terms of this Agreement, including any self-reporting described in Attachments D, E, and F, for an equivalent period.

The Defendant's Agreement

2. Pursuant to Fed. R. Crim. P. 11(c)(1)(C), the Defendant agrees to waive its right to grand jury indictment and to plead guilty to a one-count criminal Information charging the Defendant with Conspiracy to Commit Bank Fraud in violation of Title 18, United States Code, Section 1349. The Defendant further agrees to persist in that plea through sentencing and, as set forth below, to cooperate fully with the Offices in their investigation into the conduct described in this Agreement and the Statement of Facts attached hereto as Attachment A ("Statement of Facts").

3. The Defendant understands that, to be guilty of this offense, the following essential elements of the offense must be satisfied:

a. An unlawful agreement between two or more individuals to commit bank fraud, specifically, a scheme or artifice to obtain any of the moneys, funds, credits, assets,

securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises; and

b. The Defendant knowingly and willfully joined that conspiracy.

4. The Defendant understands and agrees that this Agreement is between the Offices and the Defendant and does not bind any other division or section of the Department of Justice or any other federal, state, local, or foreign prosecuting, administrative, or regulatory authority. Nevertheless, the Offices will bring this Agreement and the nature and quality of the conduct, cooperation, and remediation of the Defendant, its direct or indirect affiliates, subsidiaries, branches, and joint ventures, to the attention of other law enforcement, regulatory, and debarment authorities, if requested by the Defendant.

5. The Defendant agrees that this Agreement will be executed by an authorized corporate representative. The Defendant further agrees that a resolution duly adopted by the Defendant's Board of Directors in the form attached to this Agreement as Attachment B ("Certificate of Corporate Resolutions") authorizes the Defendant to enter into this Agreement and take all necessary steps to effectuate this Agreement, and that the signatures on this Agreement by the Defendant and its counsel are authorized by the Defendant's Board of Directors, on behalf of the Defendant.

6. The Defendant agrees that it has the full legal right, power, and authority to enter into and perform all of its obligations under this Agreement.

7. The Offices enter into this Agreement based on the individual facts and circumstances presented by this case, including:

a. The nature, seriousness, and pervasiveness of the offense conduct, as described in the Statement of Facts, including a bank fraud conspiracy in which the Defendant

misled U.S. banks in order to maintain, and in one case to open, U.S. dollar accounts that allowed the Defendant to process transactions that amounted to billions of dollars, including criminal proceeds, through the U.S. financial system and U.S. banks from accounts it opened or maintained for its high-risk, non-resident clients in Estonia from in or about 2008 to in or about January 2016 without appropriate anti-money laundering policies, procedures, and controls.

b. The Defendant did not receive voluntary disclosure credit pursuant to the United States Sentencing Guidelines ("U.S.S.G." or "Sentencing Guidelines"), because it did not voluntarily and timely disclose to the Offices the conduct described in the Statement of Facts;

c. The Defendant received credit for cooperation under U.S.S.G. § 8C2.5(g)(2), because, after becoming aware of the Offices' investigation, it provided full cooperation with the investigation and demonstrated recognition and affirmative acceptance of responsibility for its criminal conduct by, among other things, providing information obtained through its internal investigation, which allowed the government to preserve and obtain evidence as part of its own independent investigation, making regular and detailed factual presentations to the Offices, voluntarily and expediently producing a significant amount of documents located outside the United States to the Offices in ways that did not implicate foreign data privacy laws, collecting and producing voluminous evidence and information to the Offices accompanied by translations of documents, making foreign witnesses available for interviews, meeting requests from the Offices promptly, and providing detailed analysis of complex, cross-border transactions. In addition, the Defendant also provided to the Offices all relevant facts known to it, including information about the individuals involved in the conduct described in the attached Statement of Facts;

d. The Defendant engaged in remedial measures, including: (i) closing the non-resident portfolio by January 2016 as described in the Statement of Facts; (ii) terminating and separating certain employees, including senior bank executives, who were involved in the conduct; (iii) improving its overall anti-money laundering compliance function and increasing related investments and expenditures, including by establishing a centralized anti-money laundering compliance function and a financial crime program, hiring competent and experienced anti-money laundering compliance employees, and implementing new anti-money laundering compliance reporting lines directly to a member of the Defendant's Executive Leadership Team;

e. Although the Defendant had inadequate compliance programs, policies, procedures, and controls including an inadequate and ineffective anti-money laundering program (the "AML Compliance Program"), and compliance programs related to fraudulent conduct by employees, employee ethics, and whistleblowers (collectively, with the AML Compliance Program, the "Compliance Programs") during the period of the conduct described in the Statement of Facts, the Defendant has enhanced and has committed to continuing to enhance its Compliance Programs, including ensuring that its Compliance Programs satisfy the minimum elements set forth in Attachment C to this Agreement;

f. The Danish Financial Supervisory Authority ("DFSA") has appointed an independent expert selected by the DFSA to oversee the implementation of the Defendant's plan to remediate and enhance its anti-financial crime and AML functions. The Defendant has agreed to share the independent expert's reports with the Offices. To the extent the independent expert's review terminates during the Term but before the Offices have determined that the Defendant's remediation and enhancements are fully implemented and tested to demonstrate that they would

prevent and detect similar misconduct in the future, the Offices may, in their sole discretion, require the imposition of a monitor;

g. The Defendant has no prior criminal history, but it has been subject to regulatory enforcement actions related to its lack of sufficient anti-money laundering controls related to certain conduct described in the Statement of Facts, including an action by the DFSA in May 2018, which included the imposition of an independent expert in 2020 to oversee compliance remediation and enhancement;

h. The Defendant operates in a highly regulated industry, and its regulators impose capital and operating requirements;

i. The Defendant is entering into a resolution with the Securities and Exchange Commission ("SEC") relating to certain conduct described in the Statement of Facts;

j. The Defendant is entering into a resolution with authorities in Denmark relating to certain conduct described in the Statement of Facts; and

k. The Defendant has agreed to continue to cooperate with the Offices in any ongoing investigation as described in Paragraph 12 below.

l. Accordingly, after considering (a) through (k) above, the Offices believe that the appropriate resolution in this case is for the Defendant to plead guilty to one count of conspiracy to commit bank fraud pursuant to this Agreement.

8. The Defendant agrees to abide by all terms and obligations of this Agreement as described herein, including, but not limited to, the following:

a. to plead guilty as set forth in this Agreement;

b. to abide by all sentencing stipulations contained in this Agreement;

c. to appear, through its duly appointed representatives, as ordered for all court appearances, and obey any other ongoing court order in this matter, consistent with all applicable U.S. and foreign laws, procedures, and regulations;

d. to commit no further crimes;

e. to be truthful at all times with the Court;

f. to pay the applicable special assessment;

g. to consent to and to pay the applicable forfeiture amount;

h. to cooperate fully with the Offices as described in Paragraph 12;

i. to continue to implement compliance programs including the Compliance Programs as described in Paragraphs 9 and 10 and Attachment C; and

j. to provide reports from the independent expert imposed by the DFSA and self-reports as set forth in Attachment D.

9. The Defendant represents that it has implemented and will continue to implement Compliance Programs that meet, at a minimum, the elements set forth in Attachment C. Such programs shall be designed to detect and prevent violations of applicable money laundering, anti-money laundering, and bank fraud laws through the Defendant's operations, including those of its branches, subsidiaries, affiliates, agents, and joint ventures. Thirty days prior to the expiration of the Term, the Defendant, by the Chief Executive Officer and Chief Compliance Officer, will certify to the Offices, in the form of executing the document attached as Attachment F to this Agreement, that the Defendant has met its compliance obligations pursuant to this Agreement.

10. In order to address any deficiencies in its Compliance Programs, the Defendant represents that it has undertaken, and will continue to undertake in the future, in a manner consistent with all of its obligations under this Agreement, a review of its existing compliance and

ethics programs, policies, procedures, systems, and internal controls regarding compliance with money laundering and anti-money laundering laws and laws and programs related to fraudulent conduct by employees, employee ethics, and whistleblowers. Where necessary and appropriate, the Defendant agrees to adopt new or modify its Compliance Programs in order to ensure that it develops and maintains rigorous Compliance Programs, including an effective and risk-based AML Compliance Program, that incorporate relevant policies, procedures, and internal systems and controls designed to effectively detect and deter violations of money laundering, anti-money laundering, and bank fraud laws. The Compliance Programs will include, but not be limited to, the minimum elements set forth in Attachment C. The Offices, in their sole discretion, may consider the reports by the independent expert appointed pursuant to the Defendant's agreement with the DFSA in assessing the Defendant's compliance programs including the Compliance Programs.

11. Except as may otherwise be agreed by the parties in connection with a particular transaction, the Defendant agrees that in the event that, during the Term, the Defendant undertakes any change in corporate form, including if it sells, merges, or transfers business operations that are material to the Defendant's consolidated operations, or to the operations of any subsidiaries, branches, or affiliates involved in the conduct described in the Statement of Facts, as they exist as of the date of this Agreement, whether such sale is structured as a sale, asset sale, merger, transfer, or other change in corporate form, it shall include in any contract for sale, merger, transfer, or other change in corporate form a provision binding the purchaser, or any successor in interest thereto, to the obligations described in this Agreement. The purchaser or successor in interest must also agree in writing that the Offices' ability to breach under this Agreement is applicable in full force to that entity. The Defendant agrees that the failure to include these provisions in the transaction will make any such transaction null and void. The Defendant shall provide notice to the Offices at least

thirty (30) days prior to undertaking any such sale, merger, transfer, or other change in corporate form. The Offices shall notify the Defendant prior to such transaction (or series of transactions) if they determine that the transaction(s) will have the effect of circumventing or frustrating the purposes of this Agreement, as determined in the sole discretion of the Offices; the Defendant agrees that such transaction(s) will not be consummated. In addition, if at any time during the Term, the Offices determine in their sole discretion that the Defendant has engaged in a transaction(s) that has the effect of circumventing or frustrating the purposes of this Agreement, the Offices may deem it a breach of this Agreement pursuant to Paragraphs 26-28. Nothing herein shall restrict the Defendant from indemnifying (or otherwise holding harmless) the purchaser or successor in interest for penalties or other costs arising from any conduct that may have occurred prior to the date of the transaction, so long as such indemnification does not have the effect of circumventing or frustrating the purposes of this Agreement, as determined by the Offices.

12. The Defendant shall continue to cooperate fully with the Offices in any and all matters relating to the conduct described in this Agreement and the Statement of Facts and any individual or entity referred to therein, as well as any other conduct under investigation by the Offices at any time during the Term, until the later of the date upon which all investigations and prosecutions arising out of such conduct are concluded, or the end of the Term. At the request of the Offices, the Defendant shall also cooperate fully with other domestic or foreign law enforcement and regulatory authorities and agencies in any investigation of the Defendant, its subsidiaries or its affiliates, or any of its present or former officers, directors, employees, agents, and consultants, or any other party, in any and all matters relating to the conduct described in this Agreement and the Statement of Facts and other conduct under investigation by the Offices at any time during the Term. The Defendant's cooperation pursuant to this Paragraph is subject to

applicable law and regulations, including data privacy and national security laws, as well as valid claims of attorney-client privilege or attorney work product doctrine; however, the Defendant must provide to the Offices a log of any information or cooperation that is not provided based on an assertion of law, regulation, or privilege, and the Defendant bears the burden of establishing the validity of any such assertion. The Defendant agrees that its cooperation pursuant to this paragraph shall include, but not be limited to, the following, subject to local law and regulations, including relevant data privacy and national security laws and regulations:

a. The Defendant represents that it has truthfully disclosed all factual information with respect to its activities, those of its subsidiaries and affiliates, and those of its present and former directors, officers, employees, agents, and consultants relating to the conduct described in this Agreement and the Statement of Facts, as well as any other conduct under investigation by the Offices at any time about which the Defendant has any knowledge. The Defendant further agrees that it shall timely and truthfully disclose all information with respect to its activities, those of its subsidiaries and affiliates, and those of its present and former directors, officers, employees, agents, and consultants, including any evidence or allegations and internal or external investigations, about which the Offices may inquire. This obligation of truthful disclosure includes, but is not limited to, the obligation of the Defendant to provide to the Offices, upon request, any document, record, or other tangible evidence about which the Offices may inquire of the Defendant, including evidence that is responsive to any requests made prior to the execution of this Agreement.

b. Upon request of the Offices, the Defendant shall designate knowledgeable employees, directors, officers, agents, consultants, or attorneys to provide to the Offices the information and materials described in Paragraph 12 above on behalf of the Defendant. It is further

understood that the Defendant must at all times provide complete, truthful, and accurate information.

c. The Defendant shall use its best efforts to make available for interviews or testimony, as requested by the Offices, present or former officers, directors, employees, agents, and consultants of the Defendant. This obligation includes, but is not limited to, sworn testimony before a federal grand jury or in federal trials, as well as interviews with domestic or foreign law enforcement and regulatory authorities. Cooperation under this Paragraph shall include identification of witnesses who, to the knowledge of the Defendant, may have material information regarding the matters under investigation.

d. With respect to any information, testimony, documents, records, or other tangible evidence provided to the Offices pursuant to this Agreement, the Defendant consents to any and all disclosures, subject to applicable law and regulations, to other governmental authorities including United States authorities and those of a foreign government of such materials as the Offices, in their sole discretion, shall deem appropriate.

13. In addition to the obligations provided for in Paragraph 12 of the Agreement, during the Term, should the Defendant learn of any evidence or allegation of conduct that may constitute a violation of federal money laundering laws, the Bank Secrecy Act or other anti-money laundering laws, U.S. sanctions laws, or federal bank fraud laws had the conduct occurred within the jurisdiction of the United States, the Defendant shall promptly report such evidence or allegation to the Offices in a manner and form consistent with local law. Thirty days prior to the end of the Term, the Defendant, by the Chief Executive Officer of the Defendant and the Chief Financial Officer of the Defendant, will certify to the Offices, in the form of executing the document attached as Attachment E to this Agreement, that the Defendant has met its disclosure obligations pursuant

to this Paragraph. Each certification will be deemed a material statement and representation by the Defendant to the executive branch of the United States for purposes of 18 U.S.C. §§ 1001 and 1519, and it will be deemed to have been made in the judicial district in which this Agreement is filed.

14. The Defendant agrees that any fine or restitution imposed by the Court will be due and payable as specified in Paragraph 22 below, and that any restitution imposed by the Court will be due and payable in accordance with the Court's order. The Defendant further agrees to pay the Clerk of the Court for the United States District Court for the Southern District of New York the mandatory special assessment of $400 within ten business days from the date of sentencing.

The United States' Agreement

15. In exchange for the guilty plea of the Defendant and the complete fulfillment of all of its obligations under this Agreement, the Offices agree they will not file additional criminal charges against the Defendant or any of its direct or indirect affiliates, subsidiaries, or joint ventures relating to the conduct described in the Statement of Facts or the Information filed pursuant to this Agreement. The Offices, however, may use any information related to the conduct described in the Statement of Facts against the Defendant: (a) in a prosecution for perjury or obstruction of justice; (b) in a prosecution for making a false statement; (c) in a prosecution or other proceeding relating to any crime of violence; or (d) in a prosecution or other proceeding relating to a violation of any provision of Title 26 of the United States Code. This Agreement does not provide any protection against prosecution for any future conduct by the Defendant or any of its direct or indirect affiliates, subsidiaries, officers, directors, employees, agents, or consultants, whether or not disclosed by the Defendant pursuant to the terms of this Agreement. This Agreement does not provide any protection against prosecution of any individuals, regardless of

their affiliation with the Defendant. The Defendant agrees that nothing in this Agreement is intended to release the Defendant from any and all of the Defendant's tax liabilities and reporting obligations for any and all income not properly reported and/or legally or illegally obtained or derived.

Factual Basis

16. The Defendant is pleading guilty because it is guilty of the charge contained in the Information. The Defendant admits, agrees, and stipulates that the factual allegations set forth in the Information and the Statement of Facts are true and correct, that it is responsible for the acts of its officers, directors, employees, and agents described in the Information and Statement of Facts, and that the Information and Statement of Facts accurately reflect the Defendant's criminal conduct. The Defendant stipulates to the admissibility of the Statement of Facts in any proceeding by the Offices, including any trial, guilty plea, or sentencing proceeding, and will not contradict anything in the attached Statement of Facts at any such proceeding.

The Defendant's Waiver of Rights, Including the Right to Appeal

17. Federal Rule of Criminal Procedure 11(f) and Federal Rule of Evidence 410 limit the admissibility of statements made in the course of plea proceedings or plea discussions in both civil and criminal proceedings, if the guilty plea is later withdrawn. The Defendant expressly warrants that it has discussed these rules with its counsel and understands them. Solely to the extent set forth below, the Defendant voluntarily waives and gives up the rights enumerated in Federal Rule of Criminal Procedure 11(f) and Federal Rule of Evidence 410. The Defendant agrees that, effective as of the date the Defendant signs this Agreement, it will not dispute the Statement of Facts set forth in this Agreement, and that the Statement of Facts shall be admissible against the Defendant in any criminal case involving MLARS and/or the USAO-SDNY and the Defendant,

as: (a) substantive evidence offered by the government in its case-in-chief and rebuttal case; (b) impeachment evidence offered by the government on cross-examination; and (c) evidence at any sentencing hearing or other hearing. In addition, the Defendant also agrees not to assert any claim under the Federal Rules of Evidence (including Rule 410 of the Federal Rules of Evidence), the Federal Rules of Criminal Procedure (including Rule 11 of the Federal Rules of Criminal Procedure), or the United States Sentencing Guidelines (including U.S.S.G. § 1B1.1(a)) that the Statement of Facts should be suppressed or is otherwise inadmissible as evidence (in any form). Specifically, the Defendant understands and agrees that any statements that it makes in the course of its guilty plea or in connection with the Agreement are admissible against it for any purpose in any U.S. federal criminal proceeding if, even though the Offices have fulfilled all of their obligations under this Agreement and the Court has imposed the agreed-upon sentence, the Defendant nevertheless withdraws its guilty plea.

18. The Defendant is satisfied that the Defendant's attorneys have rendered effective assistance. The Defendant understands that by entering into this Agreement, the Defendant surrenders certain rights as provided in this Agreement. The Defendant understands that the rights of criminal defendants include the following:

(a) the right to plead not guilty and to persist in that plea;

(b) the right to a jury trial;

(c) the right to be represented by counsel – and if necessary have the court appoint counsel – at trial and at every other stage of the proceedings;

(d) the right at trial to confront and cross-examine adverse witnesses, to be protected from compelled self-incrimination, to testify and present evidence, and to compel the attendance of witnesses; and

(e) pursuant to Title 18, United States Code, Section 3742, the right to appeal the sentence imposed.

Nonetheless, the Defendant knowingly waives the right to appeal or collaterally attack the conviction and any sentence at or below the statutory maximum described below (or the manner in which that sentence was determined) on the grounds set forth in Title 18, United States Code, Section 3742, or on any ground whatsoever except those specifically excluded in this Paragraph, in exchange for the concessions made by the Offices in this plea agreement. This Agreement does not affect the rights or obligations of the United States as set forth in Title 18, United States Code, Section 3742(b). The Defendant also knowingly waives the right to bring any collateral challenge challenging either the conviction, or the sentence imposed in this case. The Defendant hereby waives all rights, whether asserted directly or by a representative, to request or receive from any department or agency of the United States any records pertaining to the investigation or prosecution of this case, including without limitation any records that may be sought under the Freedom of Information Act, Title 5, United States Code, Section 552, or the Privacy Act, Title 5, United States Code, Section 552a. The Defendant waives all defenses based on the statute of limitations and venue with respect to any prosecution related to the conduct described in the Statement of Facts or the Information, including any prosecution that is not time-barred on the date that this Agreement is signed in the event that: (a) the conviction is later vacated for any reason; (b) the Defendant violates this Agreement; or (c) the plea is later withdrawn, provided such prosecution is brought within one year of any such vacatur of conviction, violation of the Agreement, or withdrawal of plea, plus the remaining time period of the statute of limitations as of the date that this Agreement is signed. The Offices are free to take any position on appeal or any other post-judgment matter. The parties agree that any challenge to the Defendant's sentence

that is not foreclosed by this Paragraph will be limited to that portion of the sentencing calculation that is inconsistent with (or not addressed by) this waiver. Nothing in the foregoing waiver of appellate and collateral review rights shall preclude the Defendant from raising a claim of ineffective assistance of counsel in an appropriate forum.

Penalty

19. The statutory maximum sentence that the Court can impose for a violation of Title 18, United States Code, Section 1349 is: a fine of $1,000,000 or twice the gross pecuniary gain or gross pecuniary loss resulting from the offense, whichever is greatest (Title 18, United States Code, Section 1349 and Title 18, United States Code, Sections 3571(c) and (d)); five years' probation (Title 18, United States Code, Section 3561(c)(1)); a mandatory special assessment of $400 (Title 18, United States Code, Section 3013(a)(2)(B)); and restitution in the amount ordered by the Court. The Court must also impose forfeiture of all property constituting, or derived from, proceeds obtained, directly or indirectly, from the offense ordered by the Court (Title 18, United States Code, Section 982). In this case, the parties agree that the gross pecuniary gain resulting from the offense is $178,600,000 and therefore, pursuant to 18 U.S.C. § 3571(d), the maximum fine that may be imposed is twice the gross gain, or approximately $357,200,000. The parties also agree that the court must order forfeiture of all property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of the commission of the offense.

Sentencing Recommendation

20. The parties agree that, pursuant to *United States v. Booker*, 543 U.S. 220 (2005), the Court must determine an advisory sentencing guideline range pursuant to the United States Sentencing Guidelines. The Court will then determine a reasonable sentence within the statutory range after considering the advisory sentencing guideline range and the factors listed in Title 18,

United States Code, Section 3553(a). The parties' agreement herein to any guideline sentencing factors constitutes proof of those factors sufficient to satisfy the applicable burden of proof. The Defendant also understands that if the Court accepts this Agreement, the parties are in agreement that the Court is bound by the sentencing provisions in Paragraph 19.

21. The Offices and the Defendant agree that a faithful application of the U.S.S.G. to determine the applicable fine range yields a base offense level of 7 and total offense level of 12 based on U.S.S.G. §§ 2B1.1(a) and (b)(10). The sentence of a fine is calculated as follows:

a. Base Fine. Based upon U.S.S.G. § 8C2.4(a)(2), the base fine is $178,600,000 (the pecuniary gain to the Defendant from the offense)

b. Culpability Score. Based upon U.S.S.G. § 8C2.5, the culpability score is 8, calculated as follows:

(a)	Base Culpability Score	5
(b)(1)	Individual within the high-level participated in, condoned, or was willfully ignorant of the offense	+ 5
(g)(2)	Cooperation, Acceptance	- 2
	TOTAL	8

Calculation of Fine Range:

Base Fine	$178,600,000
Multipliers	1.6 (min)/3.2 (max)
Fine Range	$285,760,000 (min)/ $571,250,000 (max)

22. Pursuant to Rule 11(c)(1)(C) of the Federal Rules of Criminal Procedure, the Offices and the Defendant agree that the following represents the appropriate disposition of the case:

a. Disposition. Pursuant to Fed. R. Crim. P. 11(c)(1)(C), the Offices and the Defendant agree that the appropriate disposition of this case is as set forth below, and agree to recommend jointly that the Court, at a hearing to be scheduled at an agreed upon time, impose a sentence requiring the Defendant to pay criminal forfeiture only, as set forth below.

b. Criminal Fine. The parties agree, based on the application of the U.S.S.G., that the appropriate total criminal fine is $285,760,000 ("Total Criminal Fine"). The parties agree and recommend that, based on individual facts and circumstances of this case, including but not limited to the Defendant's full cooperation and agreement to forfeit $2,059,979,050, pay disgorgement and penalty to the SEC, and pay penalty and confiscation to the Danish authorities, the Court should impose forfeiture only.

c. Criminal Forfeiture. The Defendant hereby admits that the facts set forth in the Statement of Facts establish that the sum of at least $2,059,979,050 (the "Money Judgment") is forfeitable to the United States pursuant to Title 18, United States Code, Section 982(a)(2)(A). The Offices will accept the Money Judgment in full satisfaction of criminal forfeiture, considering, among other factors, capital requirements imposed by the Defendant's regulators. The Offices agree that payments made by the Defendant in connection with its concurrent settlement of a related regulatory action brought by the SEC in the amount of $178,600,000 (the "Civil Credit") and payments made by the Defendant in connection with its concurrent settlement of a related criminal action brought by the authorities in Denmark in the amount of $672,316,404 (the "Criminal Credit") shall be credited against the Money Judgment. The Defendant therefore admits the forfeiture allegation with respect to Count One of the Information, agrees that it obtained at least $2,059,979,050, and agrees to forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(2), a sum of money equal to $2,059,979,050 in United States currency,

representing proceeds traceable to the commission of said offense (the "Money Judgment"). The Offices will accept a payment of $1,209,062,646 (the "Criminal Forfeiture Payment") in full satisfaction of the Money Judgment, which reflects the Money Judgment less the anticipated payment of the Civil Credit to the SEC and the Criminal Credit to the authorities in Denmark. The Defendant agrees that it shall make the Criminal Forfeiture Payment by wire transfer pursuant to instructions provided by the Offices no later than ten business days after entry of the judgment by the Court. It is further understood that any forfeiture of the Defendant's assets shall not be treated as satisfaction of any fine, restitution, cost of imprisonment, or any other penalty the Court may impose upon the Defendant in addition to forfeiture. The Defendant consents to the entry of the Consent Preliminary Order of Forfeiture/Money Judgment annexed hereto as Attachment G and agrees that the Consent Preliminary Order of Forfeiture/Money Judgment shall be final as to the Defendant at the time it is ordered by the Court.

d. Term of Probation. The parties agree to recommend that the Court impose a term of probation for the period of the Term of this Agreement.

e. Mandatory Special Assessment. The Defendant shall pay to the Clerk of the Court for the United States District Court for the Southern District of New York within ten days of the date of sentencing the mandatory special assessment of $400.

23. This Agreement is presented to the Court pursuant to Fed. R. Crim. P. 11(c)(1)(C). The Defendant understands that, if the Court rejects this Agreement, the Court must: (a) inform the parties that the Court rejects the Agreement; (b) advise the Defendant's counsel that the Court is not required to follow the Agreement and afford the Defendant the opportunity to withdraw its plea; and (c) advise the Defendant that if the plea is not withdrawn, the Court may dispose of the case less favorably toward the Defendant than the Agreement contemplated. The Defendant further

understands that if the Court refuses to accept any provision of this Agreement, neither party shall be bound by the provisions of the Agreement.

24. The Defendant and the Offices waive the preparation of a Pre-Sentence Investigation Report ("PSR") and intend to seek a sentencing by the Court within thirty days of the Rule 11 hearing in the absence of a PSR. The Defendant understands that the decision whether to proceed with the sentencing proceeding without a PSR is exclusively that of the Court. In the event the Court directs the preparation of a PSR, the Offices will fully inform the preparer of the PSR and the Court of the facts and law related to the Defendant's case.

Corporate Compliance Reporting

25. As described in paragraph 8(j), the Defendant agrees that it will report to the Offices annually during the Term regarding remediation and the compliance measures described in Attachment C. This reporting will be conducted in accordance with Attachment D. The Defendant also agrees to provide copies of the reports issued by the independent expert appointed by the DFSA to the Offices.

Breach of Agreement

26. If the Defendant (a) commits any felony under U.S. federal law; (b) provides in connection with this Agreement deliberately false, incomplete, or misleading information; (c) fails to cooperate as set forth in Paragraph 12 of this Agreement; (d) fails to implement a compliance program as set forth in Paragraphs 9-10 of this Agreement and Attachment C; (e) commits any acts that, had they occurred within the jurisdictional reach of the United States, would be a violation of federal bank fraud or money laundering laws, or the Bank Secrecy Act; or (f) otherwise fails specifically to perform or to fulfill completely each of the Defendant's obligations under the Agreement, regardless of whether the Offices become aware of such a breach after the Term, the

Defendant shall thereafter be subject to prosecution for any federal criminal violation of which the Offices have knowledge, including, but not limited to, the charge in the Information described in Paragraphs 2 and 3, which may be pursued by the Offices in the U.S. District Court for the Southern District of New York or any other appropriate venue. Determination of whether the Defendant has breached the Agreement and whether to pursue prosecution of the Defendant shall be in the Offices' sole discretion. Any such prosecution may be premised on information provided by the Defendant or its personnel. Any such prosecution relating to the conduct described in the Information and the attached Statement of Facts or relating to conduct known to the Offices prior to the date on which this Agreement was signed that is not time-barred by the applicable statute of limitations on the date of the signing of this Agreement may be commenced against the Defendant, notwithstanding the expiration of the statute of limitations, between the signing of this Agreement and the expiration of the Term plus one year. Thus, by signing this Agreement, the Defendant agrees that the statute of limitations with respect to any such prosecution that is not time-barred on the date of the signing of this Agreement shall be tolled for the Term plus one year. The Defendant gives up all defenses based on the statute of limitations, any claim of pre-indictment delay, or any speedy trial claim with respect to any such prosecution or action, except to the extent that such defenses existed as of the date of the signing of this Agreement. In addition, the Defendant agrees that the statute of limitations as to any violation of federal law that occurs during the term of the cooperation obligations provided for in Paragraph 12 of the Agreement will be tolled from the date upon which the violation occurs until the earlier of the date upon which the Offices are made aware of the violation or the duration of the Term plus five years, and that this period shall be excluded from any calculation of time for purposes of the application of the statute of limitations.

27. In the event the Offices determine that the Defendant has breached this Agreement, the Offices agree to provide the Defendant with written notice of such breach prior to instituting any prosecution resulting from such breach. Within thirty (30) days of receipt of such notice, the Defendant shall have the opportunity to respond to the Offices in writing to explain the nature and circumstances of such breach, as well as the actions the Defendant has taken to address and remediate the situation, which explanation the Offices shall consider in determining whether to pursue prosecution of the Defendant.

28. In the event that the Offices determine that the Defendant has breached this Agreement: (a) all statements made by or on behalf of the Defendant to the Offices or to the Court, including the Information and the Statement of Facts, and any testimony given by the Defendant before a grand jury, a court, or any tribunal, or at any legislative hearings, whether prior or subsequent to this Agreement, and any leads derived from such statements or testimony, shall be admissible in evidence in any and all criminal proceedings brought by the Offices against the Defendant; and (b) the Defendant shall not assert any claim under the United States Constitution, Rule 11(f) of the Federal Rules of Criminal Procedure, Rule 410 of the Federal Rules of Evidence, or any other federal rule that any such statements or testimony made by or on behalf of the Defendant prior or subsequent to this Agreement, or any leads derived therefrom, should be suppressed or are otherwise inadmissible. The decision whether conduct or statements of any current director, officer, employee, or any person acting on behalf of, or at the direction of, the Defendant, will be imputed to the Defendant for the purpose of determining whether the Defendant has violated any provision of this Agreement shall be in the sole discretion of the Offices.

29. The Defendant acknowledges that the Offices have made no representations, assurances, or promises concerning what sentence may be imposed by the Court if the Defendant

breaches this Agreement and this matter proceeds to judgment. The Defendant further acknowledges that any such sentence is solely within the discretion of the Court and that nothing in this Agreement binds or restricts the Court in the exercise of such discretion.

Public Statements by the Defendant

30. The Defendant expressly agrees that it shall not, through present or future attorneys, officers, directors, employees, agents, or any other person authorized to speak for the Defendant make any public statement, in litigation or otherwise, contradicting the acceptance of responsibility by the Defendant set forth above or the facts described in the Information and Statement of Facts. Any such contradictory statement shall, subject to cure rights of the Defendant described below, constitute a breach of this Agreement, and the Defendant thereafter shall be subject to prosecution as set forth in Paragraphs 26-28 of this Agreement. The decision whether any public statement by any such person contradicting a fact contained in the Information or Statement of Facts will be imputed to the Defendant for the purpose of determining whether it has breached this Agreement shall be at the sole discretion of the Offices. If the Offices determine that a public statement by any such person contradicts in whole or in part a statement contained in the Information or Statement of Facts, the Offices shall so notify the Defendant, and the Defendant may avoid a breach of this Agreement by publicly repudiating such statement(s) within five business days after notification. The Defendant shall be permitted to raise defenses and to assert affirmative claims in other proceedings relating to the matters set forth in the Information and Statement of Facts provided that such defenses and claims do not contradict, in whole or in part, a statement contained in the Information or Statement of Facts. This Paragraph does not apply to any statement made by any present or former officer, director, employee, or agent of the Defendant

in the course of any criminal, regulatory, or civil case initiated against such individual, unless such individual is speaking on behalf of the Defendant.

31. The Defendant agrees that if it or any of its direct or indirect subsidiaries or affiliates issues a press release or holds any press conference in connection with this Agreement, the Defendant shall first consult the Offices to determine (a) whether the text of the release or proposed statements at the press conference are true and accurate with respect to matters between the Offices and the Defendant; and (b) whether the Offices have any objection to the release or statement.

Complete Agreement

32. This document, including its attachments, states the full extent of the Agreement between the parties. There are no other promises or agreements, express or implied. Any modification of this Agreement shall be valid only if set forth in writing in a supplemental or revised plea agreement signed by all parties.

AGREED:

FOR DANSKE BANK A/S:

Date: 12/12-2022

By: _____

Niels Heering
Senior General Counsel, Group
Danske Bank A/S

Date: 12/12/2022

By: _____

Katherine J. Stoller, Esq.
Shearman & Sterling LLP

Samuel W. Seymour, Esq.
Sharon Cohen Levin, Esq.
Sullivan & Cromwell LLP

Counsel for Danske Bank A/S

FOR THE DEPARTMENT OF JUSTICE:

BRENT S. WIBLE
Acting Chief
Money Laundering and Asset Recovery
Section, Criminal Division
U.S. Department of Justice

_____

Patrick Gushue
Margaret A. Moeser
Trial Attorneys

DAMIAN WILLIAMS
United States Attorney
Southern District of New York
U.S. Department of Justice

_____

Tara M. La Morte
Sheb Swett
Assistant United States Attorneys

ATTACHMENT A
STATEMENT OF FACTS

The following Statement of Facts is incorporated by reference as part of the Plea Agreement between the Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section ("MLARS") and the United States Attorney's Office for the Southern District of New York (the "USAO-SDNY") (collectively, the "Offices"), and the Defendant, DANSKE BANK A/S (the "Defendant" or "DANSKE BANK"). DANSKE BANK hereby agrees and stipulates that the following facts and conclusions of U.S. law are true and accurate. Certain of the facts herein are based on information obtained from third parties by the United States through its investigation and described to DANSKE BANK. The Defendant admits, accepts, and acknowledges that it is responsible for the acts of its officers, directors, employees, and agents as set forth below. Had this matter proceeded to trial, the Defendant acknowledges that the United States would have proven beyond a reasonable doubt, by admissible evidence, the facts alleged below and set forth in the Criminal Information.

DANSKE BANK

1. DANSKE BANK, the Defendant, is the largest bank in Denmark, headquartered in Copenhagen, Denmark. DANSKE BANK offers retail and corporate banking to individual and corporate customers internationally through a number of foreign operations and branches.

2. From 2007 until June 1, 2008, DANSKE BANK offered banking services through a subsidiary in Estonia. From 2008 until 2019, DANSKE BANK operated a branch headquartered in Tallinn, Estonia (hereinafter "Danske Bank Estonia").

The Scheme

3. DANSKE BANK acquired Finland-based Sampo Bank in 2007, including Sampo Bank's large operation in Estonia. A significant part 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. DANSKE BANK knew this was a large part of Sampo Bank's Estonian business model and continued this business after acquiring Sampo Bank. The non-resident portfolio ("NRP") was, by far, Danske Bank Estonia's most lucrative business line, generating, over the life of the branch, over 50% of Danske Bank Estonia's profits. DANSKE BANK knew that many NRP customers conducted transactions in U.S. dollars, which required Danske Bank Estonia to use U.S. banks and bank accounts to process those transactions. By December 2013, 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.

4. Danske Bank Estonia had an inadequate and ineffective compliance program that applied to all customers, including the NRP. Danske Bank Estonia, through its International Banking Group ("IBG"), 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. IBG 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."

5. Danske Bank Estonia had practices and procedures that further enabled NRP customers to open accounts and conduct transactions without appropriate due diligence or monitoring, including allowing representatives to open NRP customer accounts from Russia and other countries without sending account opening documents to Danske Bank Estonia, permitting

financial intermediaries such as unregulated money services businesses located outside of Estonia to open accounts, and opening accounts with minimal due diligence or know your customer ("KYC") review.

6. By at least February 2014, as a result of internal audits, DANSKE BANK knew that some of the NRP customers were engaged in highly suspicious and potentially criminal transactions, including transactions through the United States. By the same time, DANSKE BANK also knew that Danske Bank Estonia's anti-money laundering ("AML") program and procedures did not meet the standards of DANSKE BANK's AML program and procedures and were not appropriate to meet the risks posed by the NRP.

7. DANSKE BANK NRP customers conducted significant transactions in U.S. dollars using U.S. dollar accounts that Danske Bank Estonia, with the knowledge of DANSKE BANK, maintained at various U.S. banks, including U.S. Bank 1 ("U.S. BANK 1"), U.S. Bank 2 ("U.S. BANK 2"), and U.S. Bank 3 ("U.S. BANK 3"), all federally insured financial institutions located in the Southern District of New York (collectively, the "U.S. Banks"). To open and maintain these accounts, each of the U.S. Banks required Danske Bank Estonia to provide account opening information and regular updates regarding its AML compliance program and controls, transaction monitoring, and customers and transactions. The U.S. Banks also required DANSKE BANK to provide information regarding DANSKE BANK and Danske Bank Estonia.

8. The U.S. Banks further required DANSKE BANK and Danske Bank Estonia to respond to periodic inquiries regarding particular transactions or customers. Indeed, the U.S. Banks periodically made inquiries regarding suspicious transactions or suspicious customers whose transactions Danske Bank Estonia processed through the U.S. Banks.

9. The information the U.S. Banks sought was material to the U.S. Banks' decision to maintain, and in the case of U.S. Bank 3, to open, U.S. dollar accounts for Danske Bank Estonia. DANSKE BANK and Danske Bank Estonia understood that the information provided in response to such inquiries was material, that the U.S. Banks expected honest, accurate, and complete responses, and that the U.S. Banks would not open or maintain Danske Bank Estonia's U.S. dollar accounts without this information. These U.S. dollar accounts were critical to servicing NRP customers, who relied on access to the U.S. financial system via Danske Bank Estonia. In response to the requests from the U.S. Banks, DANSKE BANK misrepresented the state of Danske Bank Estonia's AML compliance program, transaction monitoring, and information regarding Danske Bank Estonia's customers and their risk profile, causing the U.S. Banks to maintain accounts, and U.S. Bank 3 to open an account, through which Danske Bank Estonia facilitated approximately $160 billion in transactions on behalf of its NRP customers between 2007 and 2016.

DANSKE BANK Identified Problems with the NRP

Regulators Brought NRP Concerns to DANSKE BANK

10. From the time DANSKE BANK purchased Sampo Bank in 2007 through at least December 2013, DANSKE BANK knew that regulators had concerns regarding the NRP and Danske Bank Estonia's business and AML practices. In 2007, the Central Bank of Russia ("CBR") sent a letter to DANSKE BANK that reported Danske Bank Estonia conducted transactions of "doubtful origin" related to customers "offshore and in the UK" that amounted to billions of rubles per month. The CBR explained that, while these transactions looked like payments for goods, those goods never crossed borders, and it was, according to the CBR, "quite obvious that neither the goods nor securities nor services do exist in reality." The CBR concluded that "the mentioned

transactions … can be connected with the criminal activity in its pure form, including money laundering."

11. Also in 2007, the Estonian Financial Supervisory Authority ("EFSA") issued a report criticizing Danske Bank Estonia's AML activities. Specifically, the report found that Danske Bank Estonia's policies were, in themselves, "mostly in compliance" with legal requirements under Estonian law; however, Danske Bank Estonia only "formally" adhered to these policies, and many aspects of its actual oversight for NRP clients were inadequate. In September 2007, the EFSA issued a precept directing Danske Bank Estonia to take a series of corrective actions to obtain better information about beneficial owners and the source of funds for the NRP. A subsequent EFSA examination in 2009 noted improvements, but it also highlighted persistent deficiencies in Danske Bank Estonia's KYC/AML policies. DANSKE BANK received copies or summaries of these examination reports.

12. When DANSKE BANK acquired Sampo Bank, it undertook a project to bring the Baltic branches onto the central technology system DANSKE BANK had established, recognizing that there were some risks, including AML risks, presented by allowing the Baltic branches to remain outside of the information technology ("IT") platform used by DANSKE BANK headquarters (the "Group"). Centralizing Danske Bank Estonia with DANSKE BANK's Group-wide IT platform would have allowed DANSKE BANK to directly monitor and/or conduct additional direct oversight of Danske Bank Estonia transactions and customers, including NRP customers and transactions Danske Bank Estonia processed through the U.S. Banks.

13. In 2008, DANSKE BANK cancelled the migration to the central technology system because the Executive Board, consisting of DANSKE BANK senior executives, concluded it would "simply be too expensive" and could cause irregularities. At a meeting of the Executive

Board where this cancellation was announced, the minutes noted that the Board members understood that it was "important that we display additional initiative in the area of compliance in consequence of our decision not to convert our Baltic banks, it is important that we make an extra effort in the compliance area." After the cancellation, Danske Bank Estonia remained on its own technology platform.

14. In 2012, the EFSA sent the Danish Financial Supervisory Authority ("DFSA") a letter that highlighted concerns with Danske Bank Estonia's AML controls. The DFSA shared these concerns with DANSKE BANK and noted that the EFSA had concluded that Danske Bank Estonia conducted a disproportionate amount of the non-resident business in Estonia. The DFSA explained that the EFSA had raised these concerns with Danske Bank Estonia without significant changes at the branch. DANSKE BANK executives, including the former Head of Group Compliance and AML ("Compliance Executive-1"), immediately asked Danske Bank Estonia executives about prior responses to the EFSA, the reason for Danske Bank Estonia's "high market share of the mentioned high -risk customers," any special KYC procedures for those high-risk customers, and how Danske Bank Estonia monitored transactions for high risk customers to minimize AML risks. The DFSA inquiry also prompted DANSKE BANK executives to revisit the 2007 CBR communication and a summary of the EFSA's 2009 examination of Danske Bank Estonia.

15. Danske Bank Estonia employees, including the former Branch Manager of Danske Bank Estonia ("Branch Manager-1") and the former Head of AML at Danske Bank Estonia ("Estonia Compliance Executive-1"), prepared a memo for DANSKE BANK senior executives that identified the NRP as a "prudent and well organized" business. The memo acknowledged that the NRP customers were high risk but claimed that Danske Bank Estonia did not open any accounts

for clients whose business activity was not "understandable." The memo included a description of both the NRP's purportedly robust onboarding procedures—noting that customers had to be approved by the "Client Committee" ("CLICO"), which Estonia Compliance Executive-1 headed—and automated transaction monitoring procedures. These representations were not true; though the CLICO and other procedures existed on paper, in 2014 Danske Bank Estonia's regulator found that there was "no evidence" that Danske Bank Estonia followed its written procedures—including onboarding procedures—or reviewed those procedures to ensure they were compliant with law and working as intended.

16. In a letter responding to the DFSA, Compliance Executive-1 repeated many of the statements contained in the Danske Bank Estonia memo, without taking any steps to confirm whether the representations in the memo were accurate or implemented in practice or whether the EFSA's findings of serious deficiencies in Danske Bank Estonia's AML program had been appropriately addressed. In particular, in a letter signed by Compliance Executive-1 and the former Head of Group Legal, DANSKE BANK informed the DFSA that DANSKE BANK was "very aware of risks being increased" as a result of the NRP customers and indicated that Danske Bank Estonia had adapted its monitoring procedures to address these increased risks. This was not accurate. In a follow-up communication to the DFSA signed by the former First Vice President, Group Financial Crime ("Compliance Executive-2"), more specifics were provided about the details of those monitoring procedures.

17. The DFSA continued its inquiries in April 2013, specifically sharing with DANSKE BANK's former Legal Head of Corporates and Institutions ("Internal Counsel-1") the EFSA's ongoing concerns that Danske Bank Estonia was not seriously addressing AML problems, particularly related to NRP customers. Internal Counsel-1 shared this with other DANSKE BANK

executives. On April 4, 2013, Internal Counsel-1 asked Compliance Executive-1 for a meeting to discuss "AML in the Baltics," explaining that the EFSA told the DFSA that "we are not taking their AML enquiries seriously . . . . I promised a reaction from us to the DFSA management tomorrow."

18. The DFSA brought to Internal Counsel-1's attention certain Russian customers the CBR had, according to Compliance Executive-1, "blacklisted" but who nevertheless banked with Danske Bank Estonia. Internal Counsel-1 shared her concerns with Compliance Executive-1, who discussed them with the AML team, noting that "there is still some nervousness about the Russian customers in Estonia again." Compliance Executive-1 said he would direct the DFSA to the earlier 2012 memo DANSKE BANK had provided. Compliance Executive-2 responded that this "is actually a bit worrying. It may prove inadequate to refer to our previous memo. So should we try to clarify what it is more specifically that they are dissatisfied with or insecure about in Estonia?" Compliance Executive-1 responded that, according to the DFSA, the "problem" was that Branch Manager-1 "brushed off the EFSA. We have blacklisted Russian customers, but are arguing that their transfers are made through a Russian bank, so what's the problem!!"

19. On April 5, 2013, Internal Counsel-1 responded to the DFSA explaining that there was a "very special setup [for] Russian customers we have in Estonia, for the very reason that these customers involve a high risk." She indicated that she had not known that the CBR had raised concerns about certain Russian customers at Danske Bank Estonia, but that Compliance Executive-1 would take action immediately. On April 7, 2013, Compliance Executive-1 told other executives in Denmark and Estonia that the EFSA had the impression that DANSKE BANK was not taking the EFSA's concerns "very seriously" and that the DFSA was "now very worried because they have confirmed to the US authorities that we comply with the Danish FSA's requirements on

AML." Compliance Executive-1 explained to other executives that it was "critical for the Bank that we do not get any problems based on this issue. We cannot risk any new orders in the AML area." On the same day, Compliance Executive-1 asked Branch Manager-1 to prepare additional information for a response to the DFSA regarding any additional conclusions related to the EFSA's concerns. Branch Manager-1 proposed a meeting with the EFSA, and a meeting was held with the EFSA on April 25, 2013. At this meeting, the EFSA recognized "that the Bank's internal AML regulations are in compliance with the established requirements," but also pointed out that "risk appetite in Estonian Danske A/S looks above the average comparing with Estonian banking sector in general." Notes of this meeting were reviewed by the EFSA and then shared with DFSA.

20. On April 8, 2013, Internal Counsel-1 told DANSKE BANK's former Chief Financial Officer ("CFO-1"), that she had confirmed that the issues the DFSA raised were correct and that Danske Bank Estonia had a deliberate policy to attract high-risk customers and was banking many high-risk customers, including a significant number of customers residing in Russia. She noted that the "business" was "fully aware" of the high-risk nature of the customers and "have established a particularly strict AML set-up in Estonia, exactly because of these customers." However, she also noted that there was new information from Estonia that "certain customers are actually blacklisted in Russia" but that "we have seen no proof of that" and that Compliance Executive-1 and a former Head of Baltic Banking (2008-2013) were looking into the issue.

21. In summer 2013, DANSKE BANK initiated a business review of the Baltic region. The then-Head of Baltic Banking (2013-2018) ("Baltic Executive-1") led the review, which concluded in a November 2013 report. The report identified certain clear red flags, including the size of the NRP and the existence of some unregulated financial intermediaries that were processing transactions through their Danske Bank Estonia accounts for unknown third parties.

The overall conclusion, however, was that the NRP had "[e]xcellent compliance processes in all aspects of the business." While the report accurately represented the size of the NRP, it contained many misstatements about Danske Bank Estonia's compliance controls.

22. After reviewing a draft of the report, Compliance Executive-2 told Compliance Executive-1 that the volume of the NRP was larger than he had previously believed and pointed out the risk of Danske Bank Estonia's relationships with unregulated intermediaries. He explained to Compliance Executive-1 that DANSKE BANK typically viewed these relationships as "extremely high risk" and the same customers would not be approved in DANSKE BANK headquarters. Compliance Executive-2 noted that many of the third-party intermediaries were not overseen by a supervisory or regulatory authority, and thus DANSKE BANK could not have "any comfort on their AML/CFT [Countering the Financing of Terrorism] procedures." As a result, if the intermediary did not do customer due diligence "very thoroughly," then DANSKE BANK could not have adequate information about the payments from the intermediary or on behalf of its customers.

23. Compliance Executive-2 stated that he "d[id] not doubt" the claimed "prudent and stable" AML environment in Danske Bank Estonia but recommended "dig[ging] deeper into the compliance and control procedures" because of the business with unregulated intermediaries and the large number of cross-border payments. Compliance Executive-2 explained that the monitoring of these intermediaries was "extremely critical in the light of the risk involved." Finally, Compliance Executive-2 noted that the EFSA had identified Danske Bank Estonia's appetite for risk as above average and called this a "very crucial piece of information which should be given serious thoughts when deciding how to proceed." Compliance Executive-2 asked Compliance Executive-1 whether DANSKE BANK wanted to be involved in such a "risky business" and

whether Danske Bank Estonia "really [has] robust monitoring procedures in place regarding these non-resident customers, covering all relevant areas in general and non-regulated entities in particular." Compliance Executive-2 felt it was "a good idea to have some 'independent' eyes" on the NRP's compliance systems.

24. Compliance Executive-1 passed along some of Compliance Executive-2's concerns to Baltic Executive-1 on October 17, 2013. In addition to sharing Compliance Executive-2's concerns, Compliance Executive-1 noted that some of these cross-border payments were likely designed to evade taxes, which would need to be reported to the authorities. DANSKE BANK did not engage "independent eyes" at this time to review the NRP or Danske Bank Estonia's compliance controls, as Compliance Executive-2 had suggested.

U.S. BANK 1 Brought NRP Concerns to the Attention of DANSKE BANK

25. U.S. BANK 1 also brought NRP concerns to the attention of Danske Bank Estonia and DANSKE BANK. As early as 2008, U.S. BANK 1 warned Danske Bank Estonia against restructuring clients' activities to avoid detection by U.S. BANK 1's transaction monitoring systems, a practice that Danske Bank Estonia had engaged in, claiming it promoted "transparency." Internally, in April 2013, U.S. BANK 1 observed that the NRP "lack[ed] transparency" and included "financial intermediaries" conducting transactions, which was a significant risk factor. In response to U.S. BANK 1's warning, Danske Bank Estonia assured U.S. BANK 1 it had taken mitigating steps, including automatic sanctions and AML monitoring, client visits, and a prohibition on third-party agents. As described in more detail below, these assurances by Danske Bank Estonia were false.

A Whistleblower Highlighted NRP Concerns
and DANSKE BANK Audit Confirmed Those Concerns

26. In a series of emails beginning in December 2013, a Whistleblower, who was a senior employee at Danske Bank Estonia, raised concerns within Danske Bank Estonia and DANSKE BANK that NRP customers were engaged in suspicious transactions and providing false account documentation, using shell companies, and potentially engaged in money laundering. The Whistleblower concluded that with respect to the NRP, Danske Bank Estonia "may itself have committed a criminal offense, . . . likely breached numerous regulatory requirements[,] [and had] a near total process failure."

27. In response, DANSKE BANK conducted two targeted internal audits in January and February 2014. After only a few days, the DANSKE BANK audit team confirmed that some NRP customers were shell companies that had false or insufficient information in Danske Bank Estonia's customer files. The DANSKE BANK audit team also determined that Danske Bank Estonia conducted almost no due diligence on the NRP customers. This contradicted prior internal audits (which had been conducted almost entirely by Danske Bank Estonia employees) and information that Danske Bank Estonia had previously provided to DANSKE BANK in response to concerns the DFSA and other regulators raised. After reviewing only a few customer files, one member of the audit team ("Auditor-1") noted that client files for certain NRP customers reflected an "unorthodox structure" and that Danske Bank Estonia relationship managers seemed to know more about the customers than was represented in the files. Auditor-1 described the results of the review as a "fire raging," concluded that customer relationships were deliberately structured to obscure beneficial owners, and was worried that the NRP accounts were being used to facilitate money laundering.

28. The DANSKE BANK internal audit team drafted a letter on February 7, 2014, that was broadly circulated among DANSKE BANK executives and confirmed that Danske Bank Estonia permitted customers with complex corporate structures, inadequate explanations for layered customer structures, and no visibility into their corporate structures, to conduct banking activities. The audit team documented significant gaps in AML practices, including insufficient transaction monitoring and Danske Bank Estonia's lack of "full information on the end-client of the Russia based intermediaries," which meant that Danske Bank Estonia was "not able to identify the actual source of funds and therefore acts against AML legislatory principles." In an audit report dated March 10, 2014, the internal audit team recommended a review of all NRP customers and Danske Bank Estonia transaction monitoring, and significant restructuring of Danske Bank Estonia AML policies and procedures.

29. Following these internal audits, DANSKE BANK commissioned an auditing firm ("Auditing Firm-1") to conduct a review of gaps in the NRP's AML/KYC processes, which was completed in April 2014. Auditing Firm-1 identified 17 shortcomings, most of which mirrored the concerns raised by the Whistleblower and identified by DANSKE BANK's internal auditors. Auditing Firm-1 confirmed that there was no automated transaction monitoring system at Danske Bank Estonia and no verification as to whether the manual transaction monitoring system was actually operating. Auditing Firm-1 also concluded that all of the NRP customers were high-risk and given the large number of such customers it was "impossible that the senior management of [IBG] could be aware of the personal circumstances of all of them," which meant that Danske Bank Estonia was "not sufficiently knowledgeable about the personal circumstance[s] of its highest risk customers to be able to manage the AML risk."

30. Compliance Executive-1 asked Auditing Firm-1 for a more qualified conclusion, and Auditing Firm-1 stated that Danske Bank Estonia had "critical gaps in the existing AML policy," including Danske Bank Estonia's failure to sufficiently document the background of on-boarded customers that left it "more susceptible to being used for money laundering." Compliance Executive-1 pressed Auditing Firm-1 for a "gut feeling" on how DANSKE BANK compared to other Baltic banks. Auditing Firm-1 replied that Danske Bank Estonia's critical gaps were "greater than we've seen in other banks in the region," and Danske Bank Estonia's peers had, by comparison, "more detailed procedures and documentation regarding decisions."

31. DANSKE BANK's response to the Whistleblower allegations, the internal audit reports, and Auditing Firm-1 report was deliberately insufficient and delayed. DANSKE BANK also did not disclose the Whistleblower allegations to any government authority or the U.S. Banks until the DFSA requested information pertaining to AML issues in Danske Bank Estonia at the end of 2017, despite the clear identification of suspicious activity within the NRP before that time. In February 2014, in-house counsel at DANSKE BANK's office in London ("Internal Counsel-2") wrote in an email to Compliance Executive-1 that his initial view was that DANSKE BANK should share the Whistleblower allegations with United Kingdom ("UK") law enforcement. Compliance Executive-1 ignored this view, and, contrary to it, told other DANSKE BANK executives that Internal Counsel-2 had said it was *not* necessary to disclose the allegations to UK law enforcement.

32. By late April 2014, Internal Counsel-2's initial view was being invoked for an even broader proposition—that it was not necessary to report to *any* authorities. DANSKE BANK executives discussed whether it was necessary to report the Whistleblower allegations to the authorities and whether to obtain outside legal advice. On April 25, 2014, Internal Counsel-1, who

did not recall speaking with Internal Counsel-2 herself about this topic, wrote to the former Chief Risk Officer ("CRO-1") that "you would like a Legal Opinion on whether we should report [the Whistleblower]'s allegations re the nonresident business and the partnership structures to the authorities. We have an internal assessment from [Internal Counsel-2] saying that we don't need to. As far as I understand it no one has started the process of getting that legal opinion yet but I will see to that next week if you still want that."

33. In 2014, DANSKE BANK executives vetoed an independent investigation that could have identified and prevented further violations of law by Danske Bank Estonia employees and customers. In May 2014, DANSKE BANK engaged a corporate investigations and security consulting firm staffed by a former law enforcement officer ("Investigative Firm-1") to investigate allegations of wrongdoing in Danske Bank Estonia. CRO-1 and the former Head of Business Banking ("Group Executive-1") objected to hiring Investigative Firm-1 because of concerns that it would lead to additional "drama," and that it was unnecessary because DANSKE BANK planned to investigate the matter internally. DANSKE BANK canceled its contract with Investigative Firm-1 and conducted only a limited internal investigation of Danske Bank Estonia customers and no investigation related to Danske Bank Estonia employees prior to public reporting about the problems in 2017.

34. In a June 2014 strategy meeting, Group Executive-1 presented a proposal to the DANSKE BANK Board of Directors to wind down the NRP in a controlled way. Other executives discussed an alternative plan to sell assets, including the profitable NRP, to another bank. The former CEO of DANSKE BANK ("CEO-1") noted that the Baltic countries were important for many of the Bank's clients and he found it unwise to speed up an exit strategy as this might significantly impact any sales price. He concluded that DANSKE BANK needed to undertake a

closer review of the business case. Group Executive-1 recalled that CEO-1 said that DANSKE BANK should proceed cautiously because there was "a lot of money" in the NRP. The Board of Directors was supportive of the proposed gradual repositioning of Danske Bank Estonia's business model, but determined that DANSKE BANK should explore all options regarding the NRP and conduct further analysis. A board member who participated in this meeting later realized the information DANSKE BANK provided the Board of Directors did not reflect the magnitude of the problems identified at Danske Bank Estonia. In 2015, there was a subsequent effort to sell the Baltic branches, including the NRP, which was ultimately unsuccessful.

35. DANSKE BANK instead opted for a gradual wind down of the NRP, allowing approximately $40 billion in additional NRP transactions through the United States from 2014 through 2016 (after the Whistleblower allegations). One internal auditor ("Auditor-2") felt senior DANSKE BANK executives pressured Auditor-2 to downplay her concerns and told her that the internal audit conclusions were "exaggerated." The former Head of International Banking ("Group Executive-2"), who was ultimately tasked with leading the response to the Whistleblower's concerns, described the NRP as a "campfire" that DANSKE BANK executives enjoyed while it was profitable but ran away from when it grew out of control.

36. In May 2014, a member of the Business Banking group told Group Executive-1: "It is my view that the local control environment, Compliance/AML and Internal Audit together with the business management (probably primarily [the Whistleblower]) have let us down big time. [The Whistleblower] was smart enough to obtain whistleblower protection for his own criminal offences, but the matter should have consequences for the other functions." Because of the deliberately slow pace of the wind-down of the NRP, DANKSE BANK did not hold employees

accountable and DANSKE BANK continued to process highly suspicious and potentially criminal transactions through the United States.

DANSKE BANK Defrauded Its U.S. Banking Partners

DANSKE BANK Misstatements to U.S. BANK 1

37. Throughout its relationship with U.S. BANK 1, Danske Bank Estonia provided false and misleading information about the NRP in response to U.S. BANK 1's inquiries. In September 2008, U.S. BANK 1 made a standard compliance visit to Danske Bank Estonia to discuss Danske Bank Estonia's compliance measures and the NRP. During those meetings, according to U.S. BANK 1's internal notes, two Danske Bank Estonia AML employees ("Estonia Compliance Employee-1" and "Estonia Compliance Employee-2," respectively) and a relationship manager ("Estonia Relationship Manager-1") made several false statements to U.S. BANK 1, including that there were no Danske Bank Estonia representative offices in Moscow, face-to-face client meetings in Estonia were required for all customers to open accounts, operations of clients were documented, and Danske Bank Estonia prohibited clients from using "dormant" UK companies, as opposed to companies that were "actively providing returns to Companies House and the equivalents."[1] The Danske Bank Estonia employees truthfully reported that when U.S. BANK 1 identified suspicious customers to Danske Bank Estonia, Danske Bank Estonia would "counsel a client to restructure to avoid catching the attention of [U.S. BANK 1's] monitoring. They encourage the client to break out their activity into two or three entities, which has the effect

[1] The Whistleblower identified multiple Danske Bank Estonia customers that were entities incorporated in the United Kingdom and moved millions of dollars through Danske Bank Estonia and the United States but reported zero income or holdings to Companies House, the UK's business registry, demonstrating that this statement was false. While Estonia Relationship Manager-1 misled U.S. BANK 1 on these issues, she also truthfully reported to U.S. Bank 1 that some Danske Bank Estonia customers were shell companies that did not want their ultimate beneficial owners ("UBOs") revealed.

of splintering the activity." This was contrary to U.S. BANK 1's prior understanding that Danske Bank Estonia closed all accounts of clients with multiple inquiries. Danske Bank Estonia employees told U.S. BANK 1 that they lacked resources to deal with the inquiries U.S. BANK 1 raised regarding suspicious transactions. The Danske Bank Estonia employees also truthfully reported that Danske Bank Estonia did not have automated transaction monitoring and instead relied on manual review of transaction reports. U.S. BANK 1 had understood that DANSKE BANK was introducing a bank-wide automated transaction monitoring solution but learned at this meeting that this effort was cancelled, which left Danske Bank Estonia with no current automated transaction monitoring solution.

38. U.S. BANK 1 concluded that this meeting "revealed a potentially significant issue with the bank counseling clients to avoid our monitoring system." As a follow-up to the meeting, U.S. BANK 1 employees emailed Danske Bank Estonia employees on November 3, 2008, stating they "were very concerned to hear that DANSKE [BANK] will work with a client to restructure their business following enquiries from correspondent banks. … We request that this practice is discontinued, if the clients request a restructuring of their business following enquiries made by [U.S. BANK 1] we ask you to alert us and forward the details of the replacement structure." U.S. BANK 1 also asked Danske Bank Estonia to keep U.S. BANK 1 updated on the "decisions and the timeframe" of the selection and implementation of an automated transaction monitoring system.

39. On November 7, 2008, U.S. BANK 1 had a follow up call with DANSKE BANK's former Head of Group Compliance and AML, former Deputy Head of Group AML, a Senior Account Manager, Estonia Compliance Employee-1, and Estonia Compliance Employee-2. During that call, the DANSKE BANK executives attempted to walk back comments Danske Bank

Estonia employees made during the September with U.S. BANK 1 by misrepresenting to U.S. BANK 1 that "Danske [Bank Estonia] does not advise clients to restructure their business after enquiries from [U.S. BANK 1]. They may advise customers that more transparency is needed in the activity. This may cause clients to divide activity into separate companies which increases transparency because one entity business would be focussed [sic] on one activity. . . . Any suspicious behaviour by clients is investigated by [Danske Bank Estonia] in Tallin." DANSKE BANK also reported that "[U.S. BANK 1] had misunderstood the [September 2008] discussions in Estonia. The group wide AML soft ware [sic] will be rolled out to all branches including the Tallinn branch. This will be rolled out at the end of 2009."

40. Based on this conversation, U.S. BANK 1 believed that Danske Bank Estonia offboarded clients of concern and did not continue to bank UBOs of those customers under different corporate structures. U.S. BANK 1 also believed that Danske Bank Estonia had a solution underway for automatic transaction monitoring. This was false. On several occasions U.S. BANK 1 flagged problematic accounts and Danske Bank Estonia closed the account referenced and simply shifted the UBO's business to other entities.

41. For example, in December 2011, U.S. BANK 1 asked Danske Bank Estonia for more information on a shell company ("Shell Company-1"), which appeared to be transacting with entities subject to U.S. sanctions. In response, Estonia Relationship Manager-1 submitted a form with additional details, including the UBO of the account. In response to U.S. BANK 1's request as to whether there was "any additional information … regarding [Shell Company-1], and/or any affiliates, to assist [U.S. BANK 1] in understanding the noted activity," Estonia Relationship Manager-1 responded "no," notwithstanding the fact that the UBO had three other accounts at Danske Bank Estonia. On February 17, 2012, U.S. BANK 1 directed Estonia Relationship

Manager-1 not to send Shell Company-1 transactions through the correspondent account, noting the entity's link to money laundering in news reports. In response, Estonia Relationship Manager-1 represented that "[w]e have been already alerted about named activity and [Shell Company-1] has no longer account with our bank." In reality, Shell Company-1 closed the account itself, and the UBO continued to bank at Danske Bank Estonia through three other shell companies, as Estonia Relationship Manager-1 knew or should have known.

42. In addition, DANSKE BANK never moved Danske Bank Estonia to the central technology system and did not tell U.S. BANK 1 that automated transaction monitoring was not implemented in Danske Bank Estonia. U.S. BANK 1 continued to meet regularly with DANSKE BANK and to ask about NRP controls and flag NRP suspicious customers or transactions. U.S. BANK 1 employees felt that Danske Bank Estonia employees responded promptly to these inquiries, though sometimes without adequate answers about the underlying purpose of relationships between counterparties. U.S. BANK 1 designated Danske Bank Estonia a high-risk client due to the NRP and the volume of alerts on NRP transactions.

43. In April 2013, Danske Bank Estonia executives met with U.S. BANK 1 employees and discussed the NRP and Danske Bank Estonia's U.S. account. U.S. BANK 1 raised concerns that the NRP "lack[ed] transparency" and included "financial intermediaries" on behalf of unidentified UBOs, both significant risk factors. Danske Bank Estonia assured U.S. BANK 1 it had taken steps to manage its risks, including automated sanctions and AML monitoring, client visits, and a prohibition on third party agents. This information was false. As an August 2014 internal Danske Bank Estonia audit memo detailed, there was no automatic AML monitoring system for Danske Bank Estonia, and such a system would not have been effective because

significant customer information was missing in Danske Bank Estonia's customer database. Danske Bank Estonia also routinely used agents in other countries to identify and onboard clients.

44. Following the April 2013 meeting with U.S. BANK 1, U.S. BANK 1 continued to raise concerns with DANSKE BANK about the high-risk NRP. Specifically, in May 2013, a U.S. BANK 1 executive ("U.S. BANK 1 Executive") reached out directly to CRO-1 to inquire about DANSKE BANK's view of the NRP. In June 2013, U.S. BANK 1 Executive met with CRO-1 and others in London. U.S. BANK 1 Executive told CRO-1 that U.S. BANK 1 expected DANSKE BANK to "reconfirm to their Estonia [branch] and to [U.S. BANK 1] that the Head office [*i.e.* DANSKE BANK headquarters] [compliance] principles would be adhered to." CRO-1 agreed and confirmed that DANSKE BANK was "compliant on both counts." This was not accurate.

45. U.S. BANK 1 Executive followed up with CRO-1, explaining that the NRP transactions Danske Bank Estonia processed through U.S. BANK 1 did not have "sufficient transparency" and thus resulted in significant suspicious activity reporting. CRO-1 discussed these concerns with Group Executive-1, among others, who concluded that U.S. BANK 1 would likely close the Danske Bank Estonia account and determined that DANSKE BANK needed to find a "plan b" for processing these transactions.

46. U.S. BANK 1 employees believed that Danske Bank Estonia offboarded customers that U.S. BANK 1 flagged as suspicious. Had the U.S. BANK 1 employees involved in the discussions with DANSKE BANK known that Danske Bank Estonia's representations regarding offboarding NRP customers and automated AML and transaction monitoring controls were false, they would have recommended exiting the relationship immediately. When one U.S. BANK 1 employee learned that Danske Bank Estonia continued to bank customer UBOs through U.S. BANK 1 using different shell companies, she felt this was "the first time in her career that she had

ever been misled in such a fashion" and, after this occurred, she changed procedures to verify in writing that offboarding included offboarding of the UBO.

47. U.S. BANK 1 Executive, who managed the DANSKE BANK relationship and coordinated the eventual closure of Danske Bank Estonia's account, understood that Danske Bank Estonia's AML and sanctions monitoring was automated. If he had known that was false, he would have "run to his boss's door to notify him" and then gone directly to U.S. BANK 1's Treasury department to "pull the plug" on the relationship. This was because the U.S. BANK 1 Executive had concluded that bank customers, especially banks in the Baltic regions, needed automatic monitoring programs or else "they would be in big trouble."

48. Because DANSKE BANK misrepresented its NRP banking practices and insufficient AML programs at Danske Bank Estonia, U.S. BANK 1 continued to bank Danske Bank Estonia. Between 2011 and 2013, Danske Bank Estonia processed $34 billion for NRP customers through its account at U.S. BANK 1.

DANSKE BANK Defrauded U.S. BANK 3

DANSKE BANK Opened the U.S. BANK 3 Account Through Fraud

49. In July 2013, senior DANSKE BANK executives worked on "plan b" to find a new U.S. banking relationship for Danske Bank Estonia because of concerns that U.S. BANK 1 would close its U.S. dollar account with Danske Bank Estonia. DANSKE BANK knew that Danske Bank Estonia needed access to the U.S. financial system to process U.S. dollar payments for the NRP and that other U.S. banks would share the same concerns that U.S. BANK 1 raised regarding the NRP. DANSKE BANK executives recognized the need to find a "long term strategy" related to the NRP.

50. At the same time, Danske Bank Estonia executives, including Branch Manager-1, discussed the need to design a strategy to "camouflage" the NRP business from DANSKE BANK executives, who were applying "great scrutiny" to the portfolio. A Danske Bank Estonia executive explained to Branch Manager-1 in an email that they had done this "exercise once before [in] 2006-2008 and we'll do it again" and noted that the "main thing is how we look in this case, not how it really is."

51. DANSKE BANK executives ultimately decided to find a new U.S. bank to handle the NRP transactions before U.S. BANK 1 closed the Danske Bank Estonia account. In July 2013, CRO-1 explained the situation to Group Executive-1 as follows: "In the short term, I think it would be preferable for us to request closure of the [U.S. BANK 1 correspondent] account (and route through other correspondents) rather than have the ignominy of their telling us. Then we need to determine future strategy before the next one drops out!"

52. U.S. BANK 1 indicated that it would no longer do business with Danske Bank Estonia but ultimately allowed Danske Bank Estonia to exit its U.S. dollar account voluntarily because U.S. BANK 1 wanted to preserve its relationship with DANSKE BANK. On August 1, 2013, Danske Bank Estonia and U.S. BANK 1 agreed that the U.S. dollar account would close within 90 days.

53. Consistent with CRO-1's email, DANSKE BANK approached U.S. BANK 3, where DANSKE BANK had an established relationship, about opening a U.S. dollar account for Danske Bank Estonia. DANSKE BANK misrepresented the reason it was seeking a new account to U.S. BANK 3 and did not inform U.S. BANK 3 of U.S. BANK 1's concerns regarding the NRP. In July 2013, a DANSKE BANK Network Manager ("Group Employee-1"), who knew that U.S. BANK 1 would no longer process NRP transactions and that Danske Bank Estonia needed a new

correspondent account for those transactions, told U.S. BANK 3 that DANSKE BANK was looking for a new Danske Bank Estonia U.S. dollar banking relationship to "concentrate[] . . . our payment flows with a limited number of providers."

54. DANSKE BANK did not indicate that U.S. BANK 1 had raised concerns about the risks associated with the NRP and was exiting the relationship with Danske Bank Estonia. According to a relationship manager at U.S. BANK 3 who managed the DANSKE BANK relationship, the fact that U.S. BANK 1 had raised concerns about Danske Bank Estonia would have been important information for U.S. BANK 3 to know before opening a U.S. dollar account for Danske Bank Estonia.

55. U.S. BANK 3 expressed interest in the account and immediately asked for "an overview of the client base" that Danske Bank Estonia served, including customers "outside Estonia," and noted U.S. BANK 3 would need "to have confirmed that [DANSKE BANK] Copenhagen Head Office ensures that the relevant AML / KYC procedures in Estonia meet the home-state standards in Denmark." Group Employee-1 immediately told DANSKE BANK's former Head of Network Management ("Bank Executive-1") that DANSKE BANK "would not be in a position to give the above [AML/KYC] confirmation to U.S. BANK 3" because Danske Bank Estonia did not have appropriate transaction monitoring. Thus, as Group Employee-1 explained, "it would not be realistic to consider [U.S. BANK 3] as an alternative provider for the USD payments from Danske [Bank] Estonia." Bank Executive-1 shared Group Employee-1's concerns and later raised concerns directly to DANSKE BANK executives, including Compliance Executive-1, Baltic Executive-1, and Branch Manager-1, noting that "if we decide to move the USD payments to [U.S. BANK 3] it is important to know that we will be required to deliver very precise information to [U.S. BANK 3] regarding the USD payments."

56. Despite understanding these concerns, Compliance Executive-1 internally confirmed that Danske Bank Estonia met home-state standards (*i.e.*, DANSKE BANK headquarters in Denmark) and could meet U.S. BANK 3's account opening requirements. On August 6, 2013, Compliance Executive-1 wrote in an internal email that Danske Bank Estonia's "AML/KYC procedures meet the home-state standards and that the standards in Estonia are specifically tailored to the customers identified as high risk customers." This was false. Indeed, in that same email Compliance Executive-1 identified internal gaps in Danske Bank Estonia's monitoring systems, such as lack of sanctions screening for incoming payments. Compliance Executive-1 justified his willingness to represent that Danske Bank Estonia met the home-state standards by noting that U.S. BANK 3's own screening mechanisms would reject payments, such as payments that violated sanctions, that Danske Bank Estonia did not block.

57. Based on this representation, Bank Executive-1 confirmed to U.S. BANK 3 on August 14, 2013, that DANSKE BANK would like to open the U.S. dollar account for Danske Bank Estonia and that Bank Executive-1 had asked the "Head of Group Compliance & Anti-Money Laundering [*i.e.*, Compliance Executive-1] to prepare a guarantee such as the one you request regarding the standard of the AML/KYC procedures of our Estonian Branch." Danske Bank Estonia employees sent U.S. BANK 3 a presentation in October 2013 that falsely stated that Danske Bank Estonia followed the KYC and AML policies and practices of DANSKE BANK, though it does not appear that Compliance Executive-1's written confirmation was ever provided to U.S. BANK 3. The presentation also contained other misrepresentations, again falsely touting the existence of an automatic monitoring system and that all non-resident customers had to meet with Danske Bank Estonia employees in person.

58. Estonia Compliance Executive-1 also knowingly misrepresented the nature of Danske Bank Estonia's business in due diligence materials he completed as part of U.S. BANK 3's account opening process. Estonia Compliance Executive-1 completed a "Correspondent Banking Client Profile Form" that U.S. BANK 3 required for new correspondent accounts. That form specifically asked Danske Bank Estonia to identify "high risk" customers; in response, Estonia Compliance Executive-1 stated that Danske Bank Estonia had no high-risk clients under Danske Bank Estonia's AML policies, even though Estonia Compliance Executive-1 had co-authored the 2012 memo explaining that Danske Bank Estonia's compliance policies were tailored to its "high market share of . . . high risk customers." Estonia Compliance Executive-1 further misrepresented that Danske Bank Estonia had no physical presence in Russia, despite Danske Bank Estonia having employees who worked out of a customer's Moscow office until 2015. Finally, Estonia Compliance Executive-1 represented that Danske Bank Estonia had "approved AML policies and procedures in place that require[d] the identification and verification of the Beneficial Ownership of [Danske Bank Estonia's] corporate customers." While there were written policies, the actual procedures Danske Bank Estonia followed were inconsistent with the written policies, as demonstrated by the Whistleblower allegations and subsequent internal audit and regulatory exams. Estonia Compliance Executive-1 made these misrepresentations despite serving as the head of the CLICO, which was, on paper, responsible for onboarding new NRP customers.

59. In October 2013, Estonia Compliance Executive-1 completed two additional forms for U.S. BANK 3 that contained more misrepresentations. U.S. BANK 3's Financial Institution Anti-Money Laundering Questionnaire contained a series of questions about Danske Bank Estonia's AML programs. On this form, Estonia Compliance Executive-1 falsely answered "yes" to the following questions:

i. Does the FI [financial institution] determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?

ii. Has the FI implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions?

iii. Does the FI complete a risk-based assessment to understand the normal and expected transactions of its customers?

60. Estonia Compliance Executive-1 knew the responses to these questions were not true. As early as 2010, Estonia Compliance Executive-1 knew that Danske Bank Estonia's financial intermediary customers were not "completely transparent" and suggested closing down those clients. However, in 2013 Danske Bank Estonia still had a number of these clients that Estonia Compliance Executive-1 had previously identified in 2010 as non-transparent, and Danske Bank Estonia had made no substantial improvements to the policies for overseeing those clients. Estonia Compliance Executive-1 did not disclose this information to U.S. BANK 3.

61. A supplemental questionnaire Estonia Compliance Executive-1 provided to U.S. BANK 3 in October 2013 also contained false and misleading information. It stated that Danske Bank Estonia employed a mixture of manual and automatic transaction monitoring, including an internally developed automatic system. Moreover, in the questionnaire Estonia Compliance Executive-1 stated that "real-time" monitoring occurred for all incoming transactions over €500,000, and that all outgoing transactions were screened against EU/UN/OFAC sanctions lists. It stated that all other monitoring occurred on daily, weekly, or monthly bases based on "certain indicators." In reality, Danske Bank Estonia had no automatic transaction monitoring system. While certain transactions over €500,000 were flagged for manual review, the 2014 EFSA audit found that manual review was entirely perfunctory and primarily handled by NRP relationship managers (Estonia Compliance Executive-1 himself sometimes reviewed these transactions as part

of his responsibilities), while the Auditing Firm-1 audit determined that manual review procedures could not be verified in practice. With respect to the review of transactions under €500,000, the EFSA found numerous instances where NRP customers engaged in transactions under the €500,000 threshold that violated Danske Bank Estonia's written policies.

62. U.S. BANK 3 relied on these various material misrepresentations and opened Danske Bank Estonia's U.S. dollar account in October 2013. Between account opening and the closure of the NRP in January 2016, DANSKE BANK processed transactions totaling approximately $3.8 billion through the U.S. BANK 3 U.S. dollar account on behalf of Danske Bank Estonia's NRP customers.

63. While DANSKE BANK was providing this information to U.S. BANK 3, DANSKE BANK executives were conducting a business review of the NRP in response to regulatory concerns, leading some DANSKE BANK executives to question whether Danske Bank Estonia conducted appropriate oversight of the NRP. By early 2014, as a result of the Whistleblower's complaints, the internal and Auditing Firm-1 audits, regulator outreach, and U.S. Bank concerns raised to DANSKE BANK, DANSKE BANK was aware of systemic KYC/AML failures, non-transparent shell company accounts, and suspicious transactions related to the NRP. DANSKE BANK did not correct any misrepresentations to U.S. BANK 3, never shared this information with U.S. BANK 3, and did not take any meaningful steps in response to these issues to stop the NRP's high-risk U.S. dollar transactions through U.S. banks.

DANSKE BANK Continued to Defraud U.S. BANK 3
As Part of the Ongoing Due Diligence on the Account

64. DANSKE BANK had several opportunities to be truthful with U.S. BANK 3 about the issues with the NRP, but instead continued to affirm and reiterate its false statements during subsequent communications with U.S. BANK 3. For example, in March 2014 a KYC Officer in

Denmark completed a questionnaire for U.S. BANK 3 providing information on "[a]ll countries where DANSKE [BANK] is represented." The answers repeated many of the false answers from previous questionnaires, including a representation that DANSKE BANK's AML policies were applied "in locations outside of [the home] jurisdiction," and that DANSKE BANK (and its branches) had "implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions."

65. In July 2014, U.S. BANK 3 employees met with Compliance Executive-2 and a Group employee to discuss the general structure of DANSKE BANK's AML program. U.S. BANK 3 employees expected Compliance Executive-2 to disclose any concerns with Danske Bank Estonia transactions at this meeting. To the contrary, Compliance Executive-2 reassured U.S. BANK 3 about the overall compliance structure of DANSKE BANK and its branches. He confirmed that whenever DANSKE BANK identified suspicious transactions involving shell companies, it sought invoices. He also did not disclose any of the serious failures DANSKE BANK and its regulators had identified regarding Danske Bank Estonia. Based on these inaccurate reassurances, U.S. BANK 3 canceled a subsequent compliance visit to Estonia after the July 2014 meeting and instead planned to review a sample of payments originating in Danske Bank Estonia to ensure they were in line with U.S. BANK 3's expectation. Compliance Executive-2 understood that U.S. BANK 3 expected truthful and accurate responses to the questions and later admitted that the answers he provided were "imprecise."

66. DANSKE BANK continued to provide misleading information to U.S. BANK 3 about Danske Bank Estonia's compliance program. In late 2014 and early 2015, U.S. BANK 3 conducted a correspondent "refresh" with Danske Bank Estonia, and DANSKE BANK coordinated the responses. Estonia Compliance Employee-2 drafted responses to a U.S. BANK 3

supplemental questionnaire in December 2014 at Compliance Executive-2's direction. This questionnaire was identical to the questionnaire Estonia Compliance Executive-1 completed in October 2013, and Estonia Compliance Employee-2 repeated the false answers Estonia Compliance Executive-1 had provided in October 2013, including misrepresentations about Danske Bank Estonia's "automatic" monitoring systems. Estonia Compliance Employee-2 also falsely stated that the automatic monitoring system had been rated "satisfactory" by internal audit.

67. U.S. BANK 3 requested, among other things, the "date and headline outcome" of Danske Bank Estonia's "last AML regulatory examination." In September 2014, the EFSA issued a preliminary report of its assessment of Danske Bank Estonia's lack of KYC and AML monitoring, which was highly critical of Danske Bank Estonia, and indicated a final report was forthcoming. The preliminary report was widely discussed by DANSKE BANK executives, with one executive noting that if only half of the EFSA report were correct, then DANSKE BANK should be moving "much faster" to shut down all non-resident business.

68. On December 12, 2014, the EFSA issued its final inspection report. Internal Counsel-1, Compliance Executive-1, and Group Executive-2 received an English translation of the summary on December 17, 2014, and Compliance Executive-2 received a copy on December 19, 2014. While the final EFSA report was less critical than the draft report, it still concluded, among other things, that Danske Bank Estonia systematically established business relationships with clients "in whose activities it is possible to see the simplest and most common suspicious circumstances" including recently established companies with no business history that operated in apartment buildings without any public facing profile. The EFSA final report explained that Danske Bank Estonia was willing to help its clients to establish accounts rather than perform independent due diligence because the economic interest in profit outweighed the performance of

due diligence required by law, that Danske Bank Estonia employees guided customers on how to avoid review of transactions, and that Danske Bank Estonia asked clients to terminate their accounts rather than cancel the account and report it as required. The EFSA report concluded that "Danske Bank [Estonia] ignores its own rules of procedure established for the prevention of money laundering and terrorist financing" and the exam "clearly proves that the rules of procedure and internal controls are not working."

69. On December 19, 2014, the same day that Compliance Executive-2 received a copy of the critical EFSA report, U.S. BANK 3 asked an employee at DANSKE BANK for more information on internal audit conclusions and regulatory review of Danske Bank Estonia.

70. The initial draft of DANSKE BANK's response, which Estonia Compliance Employee-2 prepared, answered U.S. BANK 3's questions in detail and revealed that DANSKE BANK internal auditors and outside auditors agreed that Danske Bank Estonia's AML/KYC program was severely deficient. Compliance Executive-2 edited the draft response to provide limited information to U.S. BANK 3, suggesting that Danske Bank Estonia's problems were minimal and had been remediated. Despite receiving the critical draft and final EFSA report, Compliance Executive-2, after consulting with another DANSKE BANK employee, provided the revised misleading written responses that minimized the compliance issues at Danske Bank Estonia and did not reveal the existence of the critical EFSA exam.

71. Based on the representations of Compliance Executive-2 and Estonia Compliance Employee-2, U.S. BANK 3 proceeded with the account refresh and continued to process U.S. dollar transactions for Danske Bank Estonia.

DANSKE BANK Continued to Process Transactions for Shell Companies Through U.S. BANK 3 Against U.S. BANK 3's Explicit Instructions

72. In May 2015, an officer at U.S. BANK 3 ("U.S. BANK 3 Officer") contacted Compliance Executive-2 to report suspicious payments through Danske Bank Estonia accounts. U.S. BANK 3 Officer noted, "I spoke to [Estonia Relationship Manager-1] who confirmed that these shell companies are ultimately owned by Russian individuals/Corporates who set up these shell companies to hide the fact that they are actually owned by Russians, giving them more favourable contract negotiations with global commercial trading firms." U.S. BANK 3 Officer requested that "all payments on behalf [of] any Shell Company does not get routed via Danske Bank Estonia's USD [U.S. BANK 3 account]." U.S. BANK 3 Officer recalled that neither Compliance Executive-2 nor Estonia Relationship Manager-1 raised concerns regarding his request and thus he understood that DANSKE BANK would follow the request.

73. While Compliance Executive-2 forwarded U.S. BANK 3 Officer's email internally on May 11, 2015, to numerous DANSKE BANK officials, including Bank Executive-1, DANSKE BANK ignored U.S. BANK 3's request until August 12, 2015. One DANSKE BANK executive described DANSKE BANK's inaction as "unacceptable," stating that there was a "chain break[]" in the AML Department that allowed U.S. BANK 3's request to fall through the cracks.

74. Even after DANSKE BANK delayed in reviewing U.S. BANK 3's request, it deliberately chose to ignore U.S. BANK 3's core request not to route NRP shell payments through U.S. BANK 3, and in fact increased those payments. During this same period, U.S. BANK 2 made the decision to stop processing payments through Danske Bank Estonia's U.S. dollar account. DANSKE BANK decided to reroute NRP U.S. dollar transactions that had previously gone through U.S. BANK 2 to U.S. BANK 3. DANSKE BANK executives conceded that this arrangement was directly contrary to U.S. BANK 3's no-shell request but justified it because they

were in the process of shutting down the NRP in its entirety. During these discussions, DANSKE BANK executives also revealed their concern that U.S. authorities would discover problems at DANSKE BANK, with the Executive Vice-President in Group Compliance and AML noting that "[w]e should make sure that we don't create a relationship where U.S. BANK 2 suddenly feels the need to share their concerns about [DANSKE BANK] with U.S. regulators."

75. DANSKE BANK never disclosed this decision to U.S. BANK 3. Nevertheless, DANSKE BANK unilaterally moved ahead with its plan and routed all U.S. dollar transactions, including more than $200 million in NRP transactions and suspicious shell company payments, through U.S. BANK 3 from late 2015 until the NRP was closed in January 2016. During this period, U.S. BANK 3 observed an increase in suspicious transactions that were sent through the U.S. BANK 3 account.

76. Had U.S. BANK 3 employees understood the nature and extent of DANSKE BANK and Danske Bank Estonia's misrepresentations and associated problems at the time, it would have affected their decision to open and maintain a U.S. dollar account for Danske Bank Estonia.

DANSKE BANK Closed the NRP and Ultimately Danske Bank Estonia

77. DANSKE BANK was not successful in selling the Baltic branches, including the NRP, and closed the NRP in January 2016. DANSKE BANK commissioned an internal investigation of the Estonia matter in 2017 and voluntarily made the results of the investigation public in September 2018. After some of the concerns DANSKE BANK internally identified regarding Danske Bank Estonia came to light publicly, the EFSA instructed DANSKE BANK to close Danske Bank Estonia, which DANSKE BANK completed in 2019.

78. As part of its internal investigation, and based on a review of publicly available information, DANSKE BANK determined that Danske Bank Estonia had processed through the U.S. Banks billions of dollars in transactions associated with money laundering and other criminal schemes, including Russian criminal schemes.

ATTACHMENT B
CERTIFICATE OF CORPORATE RESOLUTIONS

WHEREAS, DANSKE BANK A/S (the "Bank") has been engaged in discussions with the United States Department of Justice, Criminal Division, the Money Laundering and Asset Recovery Section and the United States Attorney's Office for the Southern District of New York (collectively, the "Offices") regarding issues arising in relation to the Offices' investigation of a violation of Title 18, United States Code, Section 1349 by certain of the Bank's employees and agents;

WHEREAS, in order to resolve such discussions, it is proposed that the Bank enter into the Plea Agreement with the Offices (the "Agreement");

WHEREAS, the Bank's Senior General Counsel, Niels Heering, together with outside counsel for the Bank, have advised the Board of Directors of the Bank of its rights, possible defenses, the Sentencing Guidelines' provisions, and the consequences of entering into such agreement with the Offices;

Therefore, the Board of Directors has RESOLVED that:

1. The Bank (a) acknowledges the filing of the one-count Information charging the Bank with a felony violation of Conspiracy to Commit Bank Fraud, in violation of Title 18, United States Code, Section 1349; (b) waives indictment on such charge and enters into the Agreement with the Offices; (c) agrees to pay a Total Criminal Forfeiture of $2,059,979,050 under the Agreement with respect to the conduct described in the Information; and (d) admits the Court's jurisdiction over the Bank and the subject matter of such action and consents to the judgment therein;

2. The Bank accepts the terms and conditions of the Agreement, including, but not

limited to: (a) a knowing waiver of its rights to a speedy trial pursuant to the Sixth Amendment to the United States Constitution, Title 18, United States Code, Section 3161, and Federal Rule of Criminal Procedure 48(b); (b) a knowing waiver, for purposes of the Agreement and any charges by the United States arising out of the conduct described in the Statement of Facts attached to the Agreement, of any objection with respect to venue, and consents to the filing of the Information, as provided under the terms of the Agreement, in the United States District Court for the Southern District of New York; and (c) a knowing waiver of any defenses based on the statute of limitations for any prosecution relating to the conduct described in the Statement of Facts attached to the Agreement and Information or relating to conduct known to the Offices prior to the date on which the Agreement is signed that is not time-barred by the applicable statute of limitations on the date of the signing of this Agreement;

3. The Bank's Senior General Counsel, Niels Heering, is hereby authorized, empowered and directed, on behalf of the Bank, to execute the Agreement substantially in such form as reviewed by this Board of Directors with such changes as the Bank's Senior General Counsel, Niels Heering, may approve;

4. The Bank's Senior General Counsel, Niels Heering, is hereby authorized, empowered, and directed to take any and all actions as may be necessary or appropriate and to approve the forms, terms, or provisions of any agreement or other documents as may be necessary or appropriate to carry out and effectuate the purpose and intent of the foregoing resolutions; and

5. All of the actions of the Bank's Senior General Counsel, Niels Heering, which actions would have been authorized by the foregoing resolutions except that such actions were taken prior to the adoption of such resolutions, are hereby severally ratified, confirmed, approved, and adopted as actions on behalf of the Bank.

Date: 12/12/22 By: _____
DANSKE BANK A/S

Date: _____ By: _____
DANSKE BANK A/S

ATTACHMENT C
COMPLIANCE COMMITMENTS

In order to address any deficiencies in its programs, policies, procedures, codes, systems, and internal controls regarding compliance with money laundering and anti-money laundering laws and fraudulent conduct by employees, employee ethics, and whistleblowers, DANSKE BANK A/S (the "Bank"), on behalf of itself and its subsidiaries, branches, and affiliates, agrees to continue to conduct, in a manner consistent with all of its obligations under this Agreement, appropriate reviews of its existing compliance programs, policies, procedures, codes, systems, and internal controls, including its anti-money laundering compliance program (the "AML Compliance Program"); and compliance programs related to fraudulent conduct by employees, employee ethics, and whistleblowers (collectively, with the AML Compliance Program, the "Compliance Programs").

Where necessary and appropriate, the Bank agrees to adopt new, or modify its existing Compliance Programs, including policies, procedures, codes, systems, and internal controls, in order to ensure that it develops and maintains rigorous, risk-based, and effective Compliance Programs that incorporate relevant policies, procedures, systems and internal controls designed to effectively detect and deter violations of money laundering, anti-money laundering, and bank fraud laws. At a minimum, this will include, but not be limited to, the following elements to the extent they are not already part of the Bank's existing Compliance Programs:

High-Level Commitment to Compliance

1. The Bank will ensure that its directors and senior management provide strong, explicit, and visible support and commitment to its Compliance Programs and demonstrate rigorous adherence by example. The Bank will also ensure that all levels of management, in turn, reinforce those standards and encourage and incentivize employees to abide by them. The Bank

will create and foster a culture of ethics and compliance with the law in its day-to-day operations at all levels of the Bank and in all lines of defense in the Compliance Programs.

Policies and Procedures

2. The Bank will maintain, or, where necessary, develop and promulgate clearly articulated and visible corporate policies against violations of money laundering, anti-money laundering, and bank fraud laws, which shall be memorialized in writing in the Compliance Programs.

3. The Bank will maintain, or, where necessary, develop and promulgate Compliance Programs designed to reduce the prospect of violations of money laundering, anti-money laundering, and bank fraud laws and the Bank's Compliance Programs, and the Bank will take appropriate measures to encourage and support the observance of ethics and the Compliance Programs by personnel at all levels of the Bank and in all lines of defense in the Compliance Programs. The Compliance Programs shall apply to all directors, officers, and employees and, where necessary and appropriate, outside parties (excluding outside counsel) acting on behalf of the Bank in a foreign jurisdiction to solicit customers or to seek new business for the Bank, including but not limited to, agents and intermediaries, consultants, representatives, distributors, teaming partners, contractors and suppliers, consortia, and joint venture partners (collectively, "agents and business partners"). The Bank shall notify all employees that compliance with the Compliance Programs is the duty of individuals at all levels of the Bank and in all lines of defense of the Compliance Programs. Such Compliance Programs shall address, at a minimum:

a. customer onboarding;

b. know your customer and due diligence procedures;

c. periodic customer reviews;

d. designation of high-risk customers;

e. high-risk customer reviews;

f. closure of customer accounts;

g. maintenance of customer files;

h. transaction monitoring;

i. filing of suspicious activity reports;

j. independent audit of AML policies, procedures, and systems;

k. conflicts of interest;

l. payments from outside sources, including but not limited to customers;

m. provision of information to U.S. correspondent banks;

n. provision of information to regulators and supervisors; and

o. whistleblowing.

Periodic Risk-Based Review

4. The Bank will maintain, or, where necessary, develop or enhance the Compliance Programs based on regular, periodic risk assessments addressing the individual circumstances of the Bank, in particular, the money laundering risks facing the Bank, 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.

5. The Bank shall review its Compliance Programs annually and update them as necessary and appropriate to ensure their continued effectiveness, taking into account relevant

developments in the field, evolving European industry standards, and the risk profile of the Bank and its customers.

Proper Oversight and Independence

6. The Bank will assign responsibility to one or more qualified senior corporate executives for the maintenance, implementation, and oversight of the Compliance Programs. Such corporate official(s) shall have the authority to report directly to independent monitoring bodies, including internal audit, external auditors, the Bank's Board of Directors, or any appropriate committee of the Bank's Board of Directors, and shall have an adequate level of autonomy from management as well as sufficient resources and authority to maintain such autonomy.

Training and Guidance

7. The Bank will maintain, or, where necessary, implement 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. These mechanisms shall include: (a) regular periodic training for all employees, including but not limited to directors and officers, all employees in positions of leadership or trust, and positions that require such training (e.g., compliance, business, internal audit, legal, finance) and, where necessary and appropriate, agents and business partners; and (b) corresponding certifications by employees certifying compliance with the training requirements. The Bank will conduct training in a manner tailored to the audience's responsibilities within the Bank, sophistication, and subject matter expertise and, where appropriate and permissible under local law, will discuss prior compliance incidents.

8. The Bank will maintain, or, where necessary, establish an effective system for providing guidance and advice to employees, including directors, officers, and, where necessary

and appropriate, agents and business partners, on complying with the Compliance Programs, including when they need advice on an urgent basis or in any foreign jurisdiction in which the Bank operates.

Internal Reporting and Investigation

9. The Bank will maintain, or, where necessary, establish an effective system for internal and, where possible, confidential reporting by, and protection of, directors, officers, employees, and, where appropriate, agents and business partners concerning violations of money laundering, anti-money laundering, and bank fraud laws; fraudulent conduct by employees; and violations of the Compliance Programs.

10. The Bank will implement mechanisms designed to ensure that the system for internal and, where possible, confidential reporting is effectively communicated to all directors, officers, employees, and, where necessary and appropriate, agents and business partners.

11. The Bank will maintain, or, where necessary, establish an effective and reliable process with sufficient resources for responding to, investigating, and documenting allegations of violations of money laundering, anti-money laundering, and bank fraud laws; fraudulent conduct by employees; and violations of the Compliance Programs.

Enforcement, Discipline, and Executive Review and Bonus Structure

12. The Bank will maintain, or, where necessary, implement mechanisms designed to effectively enforce the Compliance Programs in accordance with applicable law. Such mechanisms shall appropriately incentivize compliance and discipline violations.

13. The Bank will institute appropriate disciplinary procedures, in accordance with applicable law, to address, among other things, violations of the Compliance Programs by the Bank's directors, officers, and employees. Such procedures should be applied consistently and

fairly, regardless of the position held by, or perceived importance of, the director, officer, or employee. The Bank shall maintain, or, where necessary, implement policies and procedures to ensure that where misconduct is discovered, reasonable steps are taken to remedy the harm resulting from such misconduct, and to ensure that appropriate steps are taken to prevent further similar misconduct, including assessing the compliance policies and procedures and making modifications necessary to ensure the Compliance Programs are effective.

14. The Bank will 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. A failing score in compliance will make the executive ineligible for any bonus for that year. The Bank will include in its evaluation criteria and bonus system provisions that allow the Bank to implement measures to incentivize future compliant behavior and discipline executives for conduct occurring after the filing of the Agreement that is later determined to have contributed to future compliance failures, subject to applicable law.

Customer and Third-Party Relationships

15. The Bank will institute appropriate, risk-based know your customer, due diligence, and compliance requirements pertaining to the acceptance, retention, and oversight of all customers, agents, and business partners, including:

a. properly documented know your customer and due diligence reviews for all new customers and appropriate periodic know your customer and due diligence reviews of existing customers;

b. properly documented procedures for closing customer accounts;

c. procedures for retaining and sharing information regarding customers and transactions within the Bank and with third parties to the extent permissible by applicable law;

d. properly documented due diligence pertaining to the hiring and appropriate and regular oversight of agents and business partners;

e. informing customers of the Bank's commitment to abiding by money laundering, anti-money laundering, and bank fraud laws;

f. informing employees, and, where necessary, agents and business partners, of the Bank's commitment to abiding by money laundering, anti-money laundering, and bank fraud laws, and of the Bank's Compliance Programs; and

g. seeking a reciprocal commitment from agents and business partners.

16. Where necessary and appropriate, and in accordance with applicable law, the Bank will include standard provisions in agreements, contracts, and renewals thereof with all customers, agents, and business partners that are reasonably calculated to prevent violations of money laundering, anti-money laundering, and bank fraud laws, which may, depending upon the circumstances, include: (a) representations and undertakings relating to compliance with applicable money laundering, anti-money laundering, and bank fraud laws; (b) rights to conduct audits of the books and records of the agent, or business partner to ensure compliance with the foregoing; and (c) rights to seek termination of a customer, agent or business partner as a result of any breach of applicable money laundering, anti-money laundering, or bank fraud laws or the Bank's Compliance Programs, or the representations and undertakings related to such matters.

Mergers and Acquisitions

17. The Bank will maintain, or where necessary, develop and implement policies and procedures for mergers and acquisitions requiring that the Bank conduct appropriate risk-based

due diligence on potential new business entities, including appropriate anti-money laundering diligence by legal, accounting, and compliance personnel.

18. The Bank will ensure that the Compliance Programs apply as quickly as is practicable to newly acquired businesses or entities merged with the Bank and will promptly:

a. train the directors, officers, employees, agents, and business partners consistent with Paragraphs 7 and 8 above on the Compliance Programs;

b. ensure that any newly acquired businesses or entities are properly integrated into the Bank's existing information technology systems and subject to appropriate oversight by the Bank, including but not limited to any AML Compliance Program-related systems and any electronic communication systems or oversight; and

c. where warranted, conduct an anti-money laundering specific audit of all newly acquired or merged businesses as quickly as practicable.

Monitoring and Testing

19. The Bank will conduct periodic reviews and testing of the Compliance Programs, designed to evaluate and improve their effectiveness in preventing and detecting violations of both the Compliance Programs and money laundering, anti-money laundering, and bank fraud laws, taking into account examinations by regulators and auditors, relevant developments in the field, emerging risks, and evolving European and industry standards.

ATTACHMENT D
COMPLIANCE REPORTING REQUIREMENTS

Danske Bank A/S (the "Bank") agrees that it will report to the United States Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section and the United States Attorney's Office for the Southern District of New York (the "Offices") periodically. During the Term, as defined in Paragraph 1 of the Plea Agreement, the Bank shall review, test, and update its compliance programs, policies, procedures, codes, systems, and internal controls, including any anti-money laundering compliance program (the "AML Compliance Program"), and any compliance programs related to fraudulent conduct by employees, employee ethics, and whistleblowers (collectively, with the AML Compliance Program, the "Compliance Programs") as described in Attachment C. The Bank shall be required to: (i) conduct an initial review and submit an initial report; and (ii) conduct and prepare two follow-up reviews and reports, as described below. Prior to conducting each review, the Bank shall be required to prepare and submit a workplan for the review. The Bank shall also, at no less than three-month intervals during the Term, meet with the Offices regarding remediation, implementation, and testing of its Compliance Programs described in Attachment C.

In conducting the reviews, the Bank shall undertake the following activities, among others: (a) inspection of relevant documents, including the Bank's current policies, procedures, and training materials concerning compliance with money laundering and anti-money laundering laws, fraudulent conduct by employees, employee ethics, and whistleblowers; (b) inspection and testing of selected systems and procedures of the Bank at sample sites, including but not limited to anti-money laundering, know your customer, transaction monitoring, record-keeping, and internal audit procedures; (c) meetings with, and interviews of, relevant current and, where appropriate, former

directors, officers, employees, business partners, agents, and other persons; and (d) analyses, studies, and, most importantly, comprehensive testing of the Bank's Compliance Programs.

Written Work Plans, Reviews, and Reports

1. The Bank shall conduct an initial review and prepare an initial annual report, followed by two follow-up reviews and annual reports.

2. Within sixty (60) calendar days of the date this Agreement is executed, the Bank shall, after consultation with the Offices, prepare and submit a written work plan to address the Bank's initial review. The Offices shall have thirty (30) calendar days after receipt of the written work plan to provide comments.

3. No later than one year from the date this Agreement is executed, the Bank shall submit to the Offices a written report setting forth: (1) a complete description of its remediation efforts to date; (2) a complete description of the testing conducted to evaluate the effectiveness of the Compliance Programs and the results of that testing; and (3) proposals to ensure that its Compliance Programs are reasonably designed, implemented, and enforced so that the Compliance Programs are effective in deterring and detecting violations of money laundering, anti-money laundering laws, and bank fraud laws.

4. The Bank shall undertake two follow-up reviews and annual reports, addressing the views of the Offices on the Bank's prior reviews and reports, to further monitor and assess whether the Bank's Compliance Programs are reasonably designed, implemented, tested, and enforced so that they are effective at deterring and detecting violations of money laundering, anti-money laundering, and bank fraud laws.

5. The first follow-up annual report shall be completed by no later than one year after the initial annual report is submitted to the Offices. The second follow-up annual report shall be completed and delivered to the Offices no later than thirty (30) days before the end of the Term.

6. The Bank may extend the time period for submission of the initial annual report or any of the follow-up reports with prior written approval of the Offices.

7. With respect to each follow-up review and report, after consultation with the Offices, the Bank shall prepare a written work plan within forty-five (45) calendar days of the submission of the prior report. The Offices shall provide comments within thirty (30) calendar days after receipt of the written work plans.

8. All written work plans shall identify with reasonable specificity the activities the Bank plans to undertake to review and test each element of its Compliance Programs, as described in Attachment C.

9. Any disputes between the Bank and the Offices with respect to any written work plan shall be decided by the Offices in their sole discretion.

10. The reports and work plans shall be transmitted to:

Chief, Bank Integrity Unit
Criminal Division, Money Laundering and
Asset Recovery Section
United States Department of Justice
Criminal Division, Fraud Section
1400 New York Avenue N.W.
Washington, D.C. 20005

Chief, Money Laundering & Transnational
Criminal Enterprises Unit
United States Attorney's Office
Southern District of New York
1 Saint Andrew's Plaza
New York, New York, 10007

Meetings During the Term

11. The Bank shall meet with the Offices within thirty (30) calendar days after providing each annual report to the Offices to discuss the report.

12. At least quarterly, and more frequently if the Offices deem it appropriate in their sole discretion, representatives from the Bank and the Offices will meet to discuss the status of the review and self-reporting obligations, and any suggestions, comments, or improvements the Bank may wish to discuss with or propose to the Offices.

Provision of Reports of Third Parties and Independent Expert

13. The Bank agrees to provide the Offices with copies of any reports, not subject to a valid claim of attorney-client privilege, issued by any third party with independent oversight of either the Bank's Compliance Programs or the Bank's compliance with money laundering and anti-money laundering laws, or policies, procedures, and laws related to fraudulent conduct by employees, employee ethics, and whistleblowers. This includes, but is not limited to, reports by the independent expert appointed as part of the Bank's agreement with the Danish Financial Supervisory Authority. The Offices will have direct access to any such third party and may communicate and meet with the third party without the presence of the Bank.

Confidentiality of Submissions

14. The submissions, including the work plans and reports and any third-party reports, will likely include proprietary, financial, confidential, and competitive business information. Moreover, public disclosure of the submissions could discourage cooperation or impede pending or potential government investigations and thus undermine the objectives of the reporting requirement. For these reasons, among others, the submissions and the contents thereof are intended to remain and shall remain non-public, except as otherwise agreed to by the parties in

writing, or except to the extent the Offices determine in their sole discretion that disclosure would be in furtherance of the Offices' discharge of their duties and responsibilities or is otherwise required by law.

ATTACHMENT E
CERTIFICATION

To: United States Department of Justice
Criminal Division, Money Laundering and Asset Recovery Section
Attention: Chief, Bank Integrity Unit

United States Attorney's Office
Southern District of New York
Attention: Chief, Money Laundering and Transnational Criminal Enterprises Unit

Re: Plea Agreement Disclosure Certification

The undersigned certify, pursuant to Paragraph 13 of the Plea Agreement ("Agreement") filed on December 13, 2022 in the United States District Court for the Southern District of New York, by and between the United States Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section and the United States Attorney's Office for the Southern District of New York (the "Offices") and Danske Bank A/S (the "Bank"), that undersigned are aware of the Bank's disclosure obligations under Paragraph 13 of the Agreement and that the Bank has disclosed to the Offices any and all evidence or allegations of conduct required pursuant to Paragraph 13 of the Agreement, which includes evidence or allegations that may constitute a violation of federal money laundering laws, the Bank Secrecy Act or other anti-money laundering laws, U.S. sanctions laws, or federal bank fraud laws had the conduct occurred within the jurisdiction of the United States ("Disclosable Information"). This obligation to disclose information extends to any and all Disclosable Information that has been identified through the Bank's anti-money laundering compliance program, whistleblower channel, internal audit reports, due diligence procedures, investigation process, or other processes. The undersigned further acknowledge and agree that the reporting requirement contained in Paragraph 13 and the representations contained in this Certification constitute a significant and important component of

the Agreement and the Office's determination of whether the Bank has satisfied its obligations under the Agreement.

The undersigned hereby certify that they are respectively the Chief Executive Officer of the Bank and Chief Financial Officer of the Bank and that each has been duly authorized by the Bank to sign this Certification on behalf of the Bank.

This Certification shall constitute a material statement and representation by the undersigned and by, on behalf of, and for the benefit of, the Bank to the executive branch of the United States for purposes of 18 U.S.C. § 1001, and such material statement and representation shall be deemed to have been made in the Southern District of New York. This Certification shall also constitute a record, document, or tangible object in connection with a matter within the jurisdiction of a department and agency of the United States for purposes of 18 U.S.C. § 1519, and such record, document, or tangible object shall be deemed to have been made in the Southern District of New York.

By: _____ Dated: _____
Chief Executive Officer
Danske Bank A/S

_____
Signature

By: _____ Dated: _____
Chief Financial Officer
Danske Bank A/S

_____
Signature

ATTACHMENT F
CERTIFICATION

To: United States Department of Justice
Criminal Division, Money Laundering and Asset Recovery Section
Attention: Chief, Bank Integrity Unit

United States Department of Justice
United States Attorney's Office
Southern District of New York
Attention: Chief, Money Laundering and Transnational Criminal Enterprises Unit

Re: Plea Agreement Compliance Certification

The undersigned certify, pursuant to Paragraph 9 of the Plea Agreement ("Agreement") filed on December 13, 2022 in the United States District Court for the Southern District of New York, by and between the United States and Danske Bank A/S (the "Bank"), that the undersigned are aware of the Bank's compliance obligations under Paragraphs 9 and 10 and Attachment C of the Agreement and that, based on the undersigned's review and understanding of the Bank's compliance programs, including its anti-money laundering compliance program, the Bank has implemented compliance programs that meet the requirements set forth in Attachment C to the Agreement. The undersigned certify that the Bank's compliance programs are reasonably and effectively designed to deter and prevent violations of money laundering, anti-money laundering, and bank fraud laws throughout the Bank's operations.

The undersigned further certify that, based on a review of the Bank's reports submitted to the Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section and the United States Attorney's Office for the Southern District of New York pursuant to Paragraph 25 of the Agreement, the reports were true, accurate, and complete as of the day they were submitted.

The undersigned hereby certify that they are respectively the Chief Executive Officer of the Bank and Chief Compliance Officer of the Bank and each has been duly authorized by the Bank to sign this Certification on behalf of the Bank.

This Certification shall constitute a material statement and representation by the undersigned and by, on behalf of, and for the benefit of, the Bank to the executive branch of the United States for purposes of 18 U.S.C. § 1001, and such material statement and representation shall be deemed to have been made in the Southern District of New York. This Certification shall also constitute a record, document, or tangible object in connection with a matter within the jurisdiction of a department and agency of the United States for purposes of 18 U.S.C. § 1519, and such record, document, or tangible object shall be deemed to have been made in the Southern District of New York.

By: _____ Dated: _____
Chief Executive Officer
Danske Bank A/S

_____
Signature

By: _____ Dated: _____
Chief Compliance Officer
Danske Bank A/S

_____
Signature