



U.S. Department of Justice

*United States Attorney
District of New Jersey*

*Criminal Division
Money Laundering and Asset
Recovery Section*

*970 Broad Street, 7th floor
Newark, New Jersey 07102*

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

October 10, 2024

Loretta E. Lynch, Esq.
Paul, Weiss, Rifkind, Wharton & Garrison LLP
1285 Avenue of the Americas
New York, NY 10019

Nicolas Bourtin, Esq.
Aisling O'Shea, Esq.
Sullivan & Cromwell LLP
125 Broad Street
New York, New York 10004

Re: *United States v. TD Bank, N.A.*

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 District of New Jersey ("the USAO-DNJ") (collectively the "Offices"), and the Defendant, TD BANK, N.A. (the "Defendant," "TDBNA," 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 Toronto-Dominion Bank ("TD Bank Group"), the Defendant's global parent company, and TD Group US Holdings LLC ("TDGUS"), the intermediate holding company and U.S. parent, which are not

defendants in this matter, also agree, pursuant to the authority granted by their Boards of Directors, to certain terms and obligations of the Agreement as described below. TD Bank U.S. Holding Company (“TDBUSH”), the Defendant’s direct parent, is concurrently entering a guilty plea pursuant to authority granted by its Board of Directors. The Defendant, its parents, and all TD Bank Group’s subsidiaries, affiliates, and operations are collectively referred to as “TD ” or the Group. 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 10 below regarding 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 five years from the later of the date on which the Information is filed or the independent compliance monitor is retained by Defendant (the “Term”).

The Defendant’s Agreement

2. Pursuant to Federal Rule of Criminal Procedure 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 conspiring to: (1) fail to maintain an adequate anti-money laundering (“AML”) program, contrary to Title 31, United States Code, Sections 5318(h) and 5322, (2) fail to file accurate Currency Transaction Reports (“CTRs”), contrary to Title 31, United States Code, Sections 5313 and 5324, and (3) launder monetary instruments, contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i), in violation of Title 18, United States Code, Section 371. 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. The essential elements of conspiracy to commit an offense against the United States, as charged in the Information, are as follows:

- i. The Defendant, through its employees, made an agreement to: (1) fail to maintain an adequate AML program, (2) fail to file accurate CTRs, and (3) launder monetary instruments; and
- ii. The Defendant was a party to or member of that agreement;
- iii. The Defendant joined the agreement or conspiracy knowing of its objective and intending to join together with at least one other alleged conspirator to achieve that objective; that is, that the Defendant with at least one other alleged conspirator shared a unity of purpose and the intent to achieve that common goal or objective, to (1) fail to maintain an adequate AML program, (2) fail to file accurate CTRs, and (3) launder monetary instruments; and
- iv. At some time during the existence of the agreement or conspiracy, at least one of its members performed an overt act in order to further the objectives of the agreement.

b. The elements of the first object of the conspiracy—failure to maintain an adequate AML program—are as follows:

- i. First, the Defendant was a financial institution;
- ii. Second, the Defendant failed to establish, implement, and maintain an adequate AML program; and

- iii. Third, the Defendant acted willfully.
- c. The elements of the second object of the conspiracy—failure to file accurate CTRs—are as follows:
 - i. First, the Defendant had knowledge of the CTR reporting requirements;
 - ii. Second, the Defendant caused or attempted to cause a financial institution to file a CTR that contained a material omission or misstatement of fact; and
 - iii. Third, the Defendant acted with the purpose to evade the transaction reporting requirements.
- d. The elements of the third object of the conspiracy—laundering of monetary instruments—are as follows:
 - i. First, the Defendant transported, transmitted, or transferred a monetary instrument or funds;
 - ii. Second, the transportation, transmittal, or transfer was from a place in the United States to or through a place outside the United States or to a place inside the United States from or through a place outside the United States;
 - iii. Third, the Defendant knew that the monetary instrument or funds involved in the transportation, transmission, or transfer represented the proceeds of some form of unlawful activity; and
 - iv. Fourth, the Defendant knew that the transportation, transmission, or transfer was designed in whole or in part to conceal or disguise the

nature, the location, the source, the ownership, or the control of the proceeds of the unlawful activity.

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 prosecuting, 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 on behalf of the Defendant, and that the signatures on this Agreement by the Defendant and its counsel are authorized by the Defendant's Board of Directors.

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 and seriousness of the offense conduct, as described in the Statement of Facts, including: (a) the Defendant's pervasive and systemic failure to maintain an adequate AML compliance program, including its failure to substantively update its transaction

monitoring program from at least 2014 to 2022, its failure to monitor trillions of dollars of transactions from at least 2014 to 2024, and its failure to implement an appropriate AML compliance training program and adequately address insider risk, all of which resulted in Bank customers, sometimes aided by five Bank insiders, laundering approximately \$671 million through accounts maintained by the Defendant and created vulnerabilities that allowed the Defendant's employees to open and maintain accounts for money laundering networks that moved \$39 million in proceeds through the Defendant; (b) the Defendant's filing of 564 materially inaccurate CTRs, involving more than \$412 million in currency transactions, which omitted the identity of an individual that the Defendant knew conducted the transactions and thereby impeded law enforcement; and (c) the Defendant's conspiracy to commit money laundering, which involved five Bank employees opening accounts and conducting other account-related activities in exchange for payments that facilitated the laundering of over \$39 million in criminal proceeds from the United States to Colombia;

b. The pervasiveness of the offense, which involved the Defendant's prioritization of growth and the customer experience over compliance; implementation of a flat-cost year-over-year spending paradigm, including in its AML program, despite changing and growing AML risks; and the involvement of employees at all levels of the Defendant, ranging from store-level employees who accepted payments to open or maintain accounts involved in money laundering to senior executive management, including AML leadership, who understood the Defendant's failure to adapt its AML program to address evolving risks and the impact of the flat-cost spending paradigm for the AML program, and repeatedly failed to update and remediate the AML program, despite the Bank's consistent growth and expansion of its business in the United States;

c. The Defendant did not receive credit for voluntary self-disclosure pursuant to the Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy (“Criminal Division CEP”) or pursuant to the United States Sentencing Guidelines (“U.S.S.G.” or “Sentencing Guidelines”) § 8C2.5(g)(1) because it did not voluntarily and timely disclose to the Offices the conduct described in the Statement of Facts;

d. The Defendant received credit pursuant to U.S.S.G. § 8C2.5(g)(3) because it demonstrated recognition and affirmative acceptance of responsibility for its criminal conduct. The Defendant also received cooperation credit pursuant to the Criminal Division CEP because, after becoming aware of the Offices’ investigation, TD Bank cooperated with the investigation by, among other things: reviewing voluminous evidence produced in response to subpoenas, informal requests, and, in some cases, voluntarily identifying key information related to AML failures, money laundering, and insider activity, including information about the individuals involved in the conduct described in the Statement of Facts, which allowed the government to preserve and obtain relevant evidence; making regular and detailed factual presentations to the Offices; working with the Offices and the Bank’s regulators to ensure the production of relevant documents to the Offices; making numerous witnesses available for interviews, including witnesses located outside of the United States, and deconflicting with the Offices concerning interviews; providing relevant information related to its internal investigation, including summaries of information received from internal interviews; identifying numerous incidents of potentially suspicious activity; reviewing hundreds of hours of Bank surveillance video and identifying portions of interest to the Offices; providing detailed analyses prepared by external consultants concerning money laundering through accounts at the Defendant and the involvement of Bank employees in that conduct; and taking steps to swiftly preserve and produce records and information related to employees involved

in misconduct, including by securing their worksites to prevent the destruction of evidence. However, the Defendant's cooperation was limited in some respects, including: failing to inform the Offices of concerns expressed to the Defendant, during the course of its internal investigation, by a third-party financial services company concerning the Colombian money laundering activity and failing to identify to the Offices a well-known and significant transaction monitoring gap that, since at least 2008, allowed the Defendant to process trillions of dollars of Automated Clearing House ("ACH") and other types of transactions per year without monitoring or reporting. Additionally, the Defendant rejected requests by the government to voluntarily keep certain accounts open related to two of the three money laundering networks identified in the Statement of Facts. Therefore, the Offices determined that a discount of 20 percent of the sentence of a fine was appropriate pursuant to the Criminal Division CEP;

e. The Offices evaluated potential collateral consequences to innocent third parties, including the Defendant's employees, investors, and customers, most of whom played no role in the criminal conduct, *see* Principles of Federal Prosecution of Business Organizations, Justice Manual § 9-28.1100, as well as the remedial measures the Defendant has taken, its stated commitment to enhance its AML compliance program, and its agreement to retain an independent compliance monitor, each of which is addressed in greater detail below;

f. The Defendant has engaged and will continue to engage in significant remedial measures, which are not yet complete or fully tested, including: (i) implementing new transaction monitoring scenarios to address longstanding, known gaps in its transaction monitoring system; (ii) enhancing policies and procedures related to the identification of parties involved in conducting transactions, the collection of the conductors' identifying information, and reporting of conductors in CTRs; (iii) terminating, separating, and/or sanctioning certain employees,

including AML executives, involved in the conduct; and (iv) improving the overall AML compliance function and increasing its investments in its program, including by hiring competent and experienced AML compliance employees and executives and making significant investments in technology and AML systems;

g. The Defendant had an inadequate AML compliance program, including its policies, procedures, and controls related to transaction monitoring, identification of suspicious activity, insider risk, and employee training (collectively, the “AML Compliance Program”) during the period of the conduct described in the Statement of Facts; the Defendant has begun to enhance and committed to continue enhancing its AML Compliance Program, including, among other things, ensuring that its AML Compliance Program satisfies the minimum elements set forth in Attachment C to this Agreement;

h. The Defendant has agreed to retain an independent compliance monitor (the “Monitor”) for a period of three years (the “Term of the Monitorship”) to oversee the Defendant’s compliance remediation and enhancement and has agreed to comply with the monitorship requirements, as further described in Attachment D to this Agreement. The Offices may extend the Term of the Monitorship through the Term of the Agreement in their sole discretion. The Offices may also extend the Term of the Monitorship in the event of a breach of the Agreement;

i. The Defendant has no prior criminal history, but it was subject to regulatory enforcement actions by the Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”) and the Office of the Comptroller of the Currency (“OCC”) in September 2013 related to the Defendant’s insufficient AML controls, some of which relate to the conduct described in the Statement of Facts, as well as civil resolutions with the U.S. Securities and Exchange Commission in 2013 for unrelated conduct;

j. The Defendant has agreed to cooperate with the Offices in any investigation or prosecution as described in Paragraph 10 below;

k. The Defendant's parent company, TDBUSH, has also agreed to plead guilty and pay a criminal penalty of \$1,434,013,478.40;

l. The Defendant's global parent company, TD Bank Group, and U.S. parent company, TDGUS, have agreed to ensure that the Group cooperates with the Offices in any investigation or prosecution as described in Paragraph 10 below that the Defendant and TDBUSH meet their disclosure and compliance obligations under the Agreements, including Attachment C, by certifying to such in Attachments E and F to this Agreement and executing Attachment G to this Agreement;

m. Various components of the Group, including the Bank and TDBUSH, have agreed to enter into concurrent resolutions with the OCC, the Federal Reserve Board of Governors (the "FRB"), and FinCEN relating to certain conduct described in the Statement of Facts; and

n. Accordingly, based on consideration of (a) through (m) above, the Offices believe that a guilty plea to Count One of the Information, a criminal fine of \$500,000, and forfeiture of \$452,432,302 are sufficient but not greater than necessary to achieve the purposes described in 18 U.S.C. § 3553.

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 fine and special assessment;

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

h. to cooperate fully with the Offices as described in Paragraph 10;

i. to remediate and enhance its AML Compliance Program, as described in Paragraphs 24 and 25 and Attachment C; and

j. to retain an independent compliance Monitor to oversee implementation of the Defendant's compliance remediation and enhancement as described in Attachment D.

9. 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 transaction 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. Prior to such transaction, the purchaser or successor in interest must agree in writing that the terms and obligations of this Agreement are applicable in full force to the purchaser or successor in interest. The Defendant agrees that the

failure to include these provisions in the transaction contract will make any such transaction null and void. The Defendant shall provide notice to the Offices at least thirty 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 31–34. 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.

10. The Group shall continue to cooperate fully with the Offices in any and all matters relating to the conduct, individuals, and entities described in this Agreement and the Statement of Facts as well as any other conduct, individuals, and entities under investigation by MLARS or the USAO-DNJ 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 Group shall also cooperate fully with any other component of the Department of Justice and other domestic or foreign law enforcement and regulatory authorities and agencies in any investigation of the Defendant, its parents, 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 at any time during the Term. The Defendant's cooperation pursuant to this Agreement is subject to applicable law and regulations, including bank secrecy, 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 Agreement shall include, but not be limited to, the following:

a. The Defendant represents that it has truthfully disclosed all factual information with respect to its activities, those of its parents, 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 Group further agrees that it shall timely and truthfully disclose all information with respect to its activities, those of its parents, subsidiaries, and affiliates, and those of its present and former directors, officers, employees, agents, and consultants, including any evidence, 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 Group to provide to the Offices, upon request, any document, record, or other tangible evidence about which the Offices may inquire, including evidence that is responsive to any requests made prior to the execution of this Agreement.

b. Upon request of the Offices, the Group shall designate knowledgeable employees, directors, officers, agents, consultants, or attorneys to provide to the Offices the

information and materials described in Paragraph 10 above on behalf of the Group. It is further understood that the Group must at all times provide complete, truthful, and accurate information.

c. The Group shall use its best efforts to make available for interviews or testimony, as requested by the Offices, present and 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 Group, 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 Group consents to any and all disclosures, subject to applicable law and regulations, by the Offices 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.

11. In addition to the cooperation obligations provided for in Paragraph 10 of the Agreement, during the Term, should the Defendant learn of any evidence or allegation of conduct by the Defendant, its affiliates, or their employees that may constitute a violation of federal criminal law, 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 expiration of the Term, the Defendant, TDBUSH, TDGUS, and the Group, by the executives identified in Attachment E to this Agreement, will certify to the Offices, in the form of executing Attachment E to this Agreement, that the Defendant and its parents and affiliates have met their 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.

12. The Defendant agrees that any fine, forfeiture, or restitution imposed by the Court will be due and payable as specified in Paragraph 21 below, and that any forfeiture or restitution imposed by the Court will be due and payable in accordance with the Court's order. The Defendant further agrees to pay the mandatory special assessment of \$400 within ten business days from the date of sentencing.

The United States' Agreement

13. In exchange for the guilty plea of the Defendant and the complete fulfillment of all 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, parent companies, subsidiaries, or joint ventures relating to the conduct described in the Statement of Facts, 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 terrorism-related offense; 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, parent companies, subsidiaries, joint ventures, 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

14. The Defendant is pleading guilty because it is guilty of the charge contained in the Information. Certain of the facts are based on information obtained from third parties by the United States through its investigation and described to the Defendant. The Defendant has reviewed and verified the factual allegations. The Defendant admits, agrees, and stipulates that the factual allegations set forth in the Information and the Statement of Facts are true, accurate, 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

15. 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 and the Group and TDGUS, as represented in Attachment G, have discussed these rules with their counsel and understand 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-DNJ 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 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 the Defendant makes in the course of its guilty plea or in connection with the Agreement are admissible against the Defendant 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.

16. 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 waives its right to discovery. The Defendant further 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 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 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 Defendant further waives the right to raise on appeal or on collateral review any argument that the statutes to which the Defendant is pleading guilty are unconstitutional and/or the admitted conduct does not fall within the scope of the statutes. 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

17. The statutory maximum sentence that the Court can impose for a violation of Title 18, United States Code, Section 371, as charged in the Information, is: a fine of up to \$500,000 or twice the gross pecuniary gain or gross pecuniary loss resulting from the offense, whichever is greatest (Title 18, United States Code, Section 3571(c)(3)); five years' probation (Title 18, United States Code, Section 3561(c)(1)); and a mandatory special assessment of \$400 (Title 18, United States Code, Section 3013(a)(2)(B)); for the conspiracy to violate 31 U.S.C. §§ 5313 and 5324, forfeiture of all property, real or personal, involved in the offense and any property traceable thereto (Title 31, United States Code, Section 5317(c)(1)(A)); and for the conspiracy to violate Title 18, United States Code, Section 1956(a)(2)(B)(i), the Court must impose forfeiture to the United States of any property, real or personal, which constitutes or is derived from proceeds traceable to the conspiracy to commit such offense (Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461).

18. The parties agree that the Court should impose the statutory maximum \$500,000 fine on the Defendant. The parties further agree that the conspiracy to violate Title 31, United States Code, Sections 5313 and 5324 involved property in an amount of \$412,876,589, which is the amount that must be forfeited to the United States. The parties also agree that the conspiracy to violate Title 18, United States Code, Section 1956(a)(2)(B)(i) involved property in an amount of \$39,555,713, which is the amount that must be forfeited to the United States.

Sentencing Recommendation

19. 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 Paragraphs 17 and 18.

20. The Offices and the Defendant agree that a faithful application of the U.S.S.G. to determine the applicable fine range yields a total offense level of 38 based on U.S.S.G. §§ 2X1.1, 2S1.3, 3D1.2, and 3D1.3. The guideline calculation begins with a base offense level of 6 for the CTR-related conspiracy, U.S.S.G. §§ 2X1.1(a) and 2S1.3(a)(2); 28 levels are added based on the value of funds, U.S.S.G. § 2S1.3(a)(2); two levels are added because the Defendant knew or believed funds were proceeds of unlawful activity or were intended to promote unlawful activity, U.S.S.G. § 2S1.3(b)(1); and two levels are added because the Defendant was convicted of an offense under subchapter II of chapter 53 of title 31, United States Code and committed the offense

as part of a pattern of unlawful activity involving more than \$100,000 in a 12-month period, U.S.S.G. § 2S1.3(b)(3). The sentence of a fine is calculated as follows:

- a. Base Fine. Based upon U.S.S.G. § 8C2.4(a)(1), the base fine is \$150,000,000 (corresponding to the Defendant's offense level of 38)
- b. Culpability Score. Based upon U.S.S.G. § 8C2.5, the culpability score is 10, calculated as follows:

(a)	Base Culpability Score	5
(b)(1)	Individual within the high-level personnel participated in, condoned, or was willfully ignorant of the offense	+ 5
(c)(2)	Civil Adjudication within five years	+ 2
(g)(2)	Cooperation, Acceptance	- 2
	TOTAL	10

- c. Calculation of Fine Range:

Base Fine	\$150,000,000
Multipliers	2.0 (min)/4.0 (max)
Fine Range	\$300,000,000 (min)/ \$600,000,000 (max)

- d. Statutory Maximum Fine:

Up to \$500,000 or twice the gross pecuniary gain or gross pecuniary loss resulting from the offense, whichever is greatest (18 U.S.C. § 3571(c)(3))

21. 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 parties agree that the appropriate disposition of this case is as set forth herein, and agree to jointly recommend that

the Court, at a hearing to be scheduled at an agreed upon time, impose a sentence requiring the Defendant to pay a criminal fine and criminal forfeiture, as set forth below.

b. Criminal Fine. Considering the \$500,000 statutory maximum, the parties agree that the appropriate total criminal fine is \$500,000 (“Total Criminal Fine”). The Defendant agrees that it shall pay the Total Criminal Fine to the Court no later than ten business days after entry of the judgment by the Court.

c. Criminal Forfeiture. The Defendant hereby admits that the facts set forth in the Statement of Facts establish that the sum of \$452,432,302 (the “Money Judgment”) is forfeitable to the United States pursuant to Title 31, United States Code, Section 5317(c)(1), and Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461. The Offices will accept the Money Judgment in full satisfaction of criminal forfeiture. The Defendant admits the forfeiture allegation of the Information with respect to the second object of the conspiracy, agrees that it failed to file accurate CTRs involving property in the amount of \$412,876,589, and agrees to forfeit to the United States, pursuant to Title 31, United States Code, Section 5317(c)(1), a sum of money equal to \$412,876,589 in United States currency. The Defendant further admits the forfeiture allegation of the Information with respect to the third object of the conspiracy, agrees that the amount of proceeds traceable to such conspiracy is \$39,555,713, and agrees to forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, a sum of money equal to \$39,555,713 in United States currency. The Offices agree that payments made by the Group in connection with its concurrent settlement of a related regulatory action brought by the FRB in the amount of \$123,500,000 shall be credited against the Money Judgment. The Offices will accept a payment of \$328,932,302 (the “Criminal Forfeiture Payment”) in full satisfaction of the Money Judgment.

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

e. 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, pursuant to Title 18, United States Code, Sections 3551(c)(1) and 3561(c)(1). The Defendant will continue on probation until it has served the full five years, unless the Court approves early termination of probation. The parties agree, pursuant to U.S.S.G. § 8D1.4, that the term of probation shall include as conditions the obligations set forth in Paragraphs 8(a)–(h), and Paragraphs 21(b), (c), and (e). A condition of probation shall be that the Defendant retain a Monitor, as provided in Paragraph 7(h). However, the condition of probation is limited to the retention of the Monitor—not oversight of the Monitor or the Company's compliance with the Monitor's recommendations. The Monitor will report to and be overseen by the Offices. The Monitor's selection process, mandate, duties, review, and certification as described in Paragraphs 26–30 and Attachment D, and the Defendant's compliance obligations as described in Paragraphs 24 and 25 and Attachment C, are not conditions of

probation. In the event the Offices find, in their sole discretion pursuant to Paragraph 7(h), that there exists a change in circumstances sufficient to eliminate the need for the Monitor or extend the term of the Monitor during the term of probation, the parties will submit a joint motion to modify the special conditions of probation.

22. This Agreement is presented to the Court pursuant to Federal Rule of Criminal Procedure 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.

23. 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.

Compliance Program, Independent Compliance Monitor, and Reporting

24. The parties have agreed to the compliance, monitoring, and reporting requirements set forth in Attachments C and D. The Defendant represents that it will continue to implement and enhance its AML Compliance Program such that it meets, at a minimum, the elements set forth in Attachment C. Such programs shall be designed to detect and prevent violations of the BSA, laws

prohibiting money laundering, and other laws prohibiting illicit finance through the Defendant's operations, as defined in Attachment C. Thirty days prior to the expiration of the Term, the Defendant, by its Chief Executive Officer and BSA Officer, TD Bank Group's Chief Executive Officer and Chief AML Officer, and TDGUS's Chief Executive Officer and Chief Risk 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.

25. In order to address any deficiencies in its AML Compliance Program, 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 the BSA, laws prohibiting money laundering, and other laws prohibiting illicit finance. Where necessary and appropriate, the Defendant agrees to adopt new controls or otherwise modify its AML Compliance Program in order to ensure that it develops and maintains an effective and risk-based AML program that incorporates relevant policies, procedures, and internal systems and controls designed to effectively detect and deter violations of the BSA, laws prohibiting money laundering, and other laws prohibiting illicit finance. The AML Compliance Program will include, at a minimum, the elements set forth in Attachment C. The Offices, in their sole discretion, may consider the reports by the independent Monitor appointed pursuant to Attachment D in assessing the Defendant's AML Compliance Program.

26. Promptly after the Offices' selection pursuant to Paragraph 28 below, the Defendant agrees to retain the Monitor. The Monitor's duties and authority, and the obligations of the Defendant with respect to the Monitor and the Offices, are set forth in Attachment D, which is incorporated by reference into this Agreement. No later than thirty days after the execution of this

Agreement, the Defendant shall submit a written proposal to the Offices identifying three Monitor candidates, and, at a minimum, providing the following:

- a. A description of each candidate's qualifications and credentials in support of the evaluative considerations and factors listed below;
- b. A written certification by the Defendant that the Defendant and its subsidiaries will not employ or be affiliated with the Monitor for a period of not less than three years from the date of the termination of the monitorship;
- c. A written certification by each of the candidates that he/she is not a current or recent (i.e., within the prior two years) employee, agent, or representative of the Defendant and holds no interest in, and has no relationship with, the Defendant, its subsidiaries, affiliates, or related entities, or its employees, officers, or directors;
- d. A written certification by each of the candidates that he/she has notified any clients that the candidate represents in a matter involving the Offices (or any other Department component) handling the Monitor selection process, and that the candidate has either obtained a waiver from those clients or has withdrawn as counsel in the other matter(s); and;
- e. A statement identifying the Monitor candidate that is the Defendant's first, second, and third choice to serve as the Monitor.

27. The Monitor candidates or their team members shall have, at a minimum, the following qualifications:

- a. Demonstrated expertise with respect to the BSA and other applicable laws requiring AML programs, including experience counseling or advising on

- effective AML programs at financial institutions;
- b. Experience designing and/or reviewing corporate compliance programs, policies, procedures, and controls, including AML compliance programs and compliance programs implemented at financial institutions;
- c. The ability to access and deploy resources as necessary to discharge the Monitor's duties as described in the Agreement; and
- d. Sufficient independence from the Defendant and its subsidiaries to ensure effective and impartial performance of the Monitor's duties as described in the Agreement.

28. The Offices retain the right, in their sole discretion, to choose the Monitor from among the proposed candidates, though the Defendant may express its preference(s) among the candidates. Monitor selections shall be made in keeping with the Department's commitment to diversity and inclusion. If the Offices determine, in their sole discretion, that any of the candidates are not, in fact, qualified to serve as the Monitor, or if the Offices, in their sole discretion, are not satisfied with the candidates proposed, the Offices reserve the right to request that the Defendant nominate additional candidates. In the event the Offices reject any proposed Monitors, the Defendant shall propose additional candidates within twenty business days after receiving notice of the rejection so that three qualified candidates are proposed. This process shall continue until a Monitor acceptable to both parties is chosen. The Offices and the Defendant will use their best efforts to complete the selection process within sixty days of the execution of this Agreement. The Offices retain the right to determine that the Monitor should be removed, if in the Offices' sole discretion, the Monitor fails to conduct the monitorship effectively, fails to comply with this Agreement, or no longer meets the qualifications outlined in Paragraph 27 above. If the Monitor

resigns, is removed, or is otherwise unable to fulfill his or her obligations as set out herein and in Attachment D, the Defendant shall within twenty business days recommend a pool of three qualified Monitor candidates from which the offices will choose a replacement, following the Monitor selection process outlined above.

29. The Monitor's term shall be three years from the date on which the Monitor is retained by the Defendant, subject to extension or early termination in the Offices' sole discretion as described in Paragraph 7(h).

30. The Monitor's powers, duties, and responsibilities, as well as circumstances that may support an extension of the Monitor's term, are set forth in Attachment D. The Defendant agrees that the Defendant and its subsidiaries, parents, branches, and affiliates will not employ or be affiliated with the Monitor or the Monitor's firm for a period of not less than three years from the date on which the Monitor's term expires, nor will the Defendant and its subsidiaries, parents, branches, and affiliates discuss with the Monitor or the Monitor's firm the possibility of further employment or affiliation during the Monitor's term. Should the Defendant be required to retain an independent compliance monitor or similar person with responsibility for overseeing or evaluating the Defendant's AML Compliance Program in connection with any parallel civil or regulatory resolution, the Defendant agrees to consult with the Offices regarding the selection of that person and before retaining that person to ensure, among other things, coordination with the Monitor pursuant to this Agreement. The Offices agree that the Monitor appointed pursuant to this Agreement may also serve in such a role.

Breach of Agreement

31. 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 10 of this Agreement; (d) fails to implement a compliance program at the Defendant as set forth in Paragraphs 24 and 25 of this Agreement and Attachment C and complete the monitorship as set forth in Paragraphs 7(h) and 26–30 of this Agreement and Attachment D; (e) commits any acts that, had they occurred within the jurisdictional reach of the United States, would be a violation of federal money laundering laws or the Bank Secrecy Act; or (f) otherwise fails specifically to perform or to fulfill completely each of the obligations under the Agreement, regardless of whether the Offices become aware of such a breach after the Term, the Defendant entity 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 District of New Jersey or any other appropriate venue. Determination of whether the Defendant or TD Bank has breached the Agreement and whether to pursue prosecution of the Defendant shall be in the Offices' sole discretion. In determining a breach in the Offices' discretion, the Offices will take into consideration, among other factors, whether the Defendant voluntarily disclosed any criminal violations, its cooperation in any investigation and remediation of the conduct, the severity and pervasiveness of the conduct, and the seniority of the employees involved. 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, or the Group or TDGUS pursuant to Attachment G, 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 10 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.

32. In the event that the Offices determine there is a breach of 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 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.

33. In the event that the Offices determine there has been a breach of 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 as to 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 made in the sole discretion of the Offices.

34. 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, including whether the statutory maximum for these offenses represents the maximum penalty that could be imposed in any future prosecution of Defendant. 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 or precludes the Offices from arguing for any higher sentence.

Public Statements by the Defendant

35. The Defendant expressly agrees that it shall not, through present or future parents, affiliates, 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 31–34 of this Agreement. The decision as to 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 made in 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.

36. The Defendant agrees that if it or any of its direct or indirect subsidiaries or affiliates makes any affirmative public statement in connection with this Agreement, including via press release, press conference remarks, or a scripted statement to investors, 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

37. 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 TD BANK, N.A.:

Date: 10/10/2024

By: CBA Adams
Cynthia Adams
General Counsel
TD Bank, N.A.

Date: 10/10/2024

By: Loretta E. Lynch
Loretta E. Lynch, Esq.
Paul, Weiss, Rifkind, Wharton & Garrison
LLP

By: Nicolas Bourdin
Nicolas Bourdin, Esq.
Aisling O'Shea, Esq.
Sullivan & Cromwell LLP

Counsel for TD Bank, N.A.

FOR THE DEPARTMENT OF JUSTICE:

MARGARET A. MOESER
Chief, Money Laundering and Asset Recovery
Section
Criminal Division
U.S. Department of Justice

DZ

D-Zachary Adams
Chelsea R. Rooney
Trial Attorneys

PHILIP R. SELLINGER
United States Attorney
District of New Jersey
U.S. Department of Justice

PS

Mark J. Pesce
Angelica M. Sinopole
Assistant United States Attorneys

STATEMENT OF COUNSEL

As counsel for the Defendant, I have discussed all plea offers and the terms of this plea agreement with the Defendant, have fully explained the charge to which the Defendant is pleading guilty and the necessary elements, all possible defenses, stipulations, waivers, fine, forfeiture, sentencing, and the consequences of a guilty plea to a felony. Based on these discussions, I have no reason to doubt that the Defendant is knowingly and voluntarily entering into this agreement and entering a plea of guilty. I know of no reason to question the Defendant's competency to make these decisions. If, prior to the imposition of sentence, I become aware of any reason to question the Defendant's competency to enter into this plea agreement or to enter a plea of guilty, I will immediately inform the Court.

DATED: October 10, 2024

A handwritten signature in cursive script, appearing to read "Loretta E. Lynch", is written over a horizontal line.

LORETTA E. LYNCH
NICOLAS BOURTIN
AISLING O'SHEA

Counsel for Defendant

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 District of New Jersey (the “USAO-DNJ”) (collectively, the “Offices”), and TD BANK US HOLDING COMPANY (“TDBUSH”) and TD BANK, NATIONAL ASSOCIATION (“TDBNA” or the “Bank”) (collectively, the “Defendants”). The Defendants hereby agree and stipulate that the following facts 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 the Defendants.

The Defendants admit, accept, and acknowledge that they are responsible for the acts of their officers, directors, employees, and agents as set forth below. Had this matter proceeded to trial, the Defendants acknowledge that the United States would have proven beyond a reasonable doubt by admissible evidence the facts alleged below and set forth in the Criminal Informations.

Overview

1. TDBNA, which markets itself as “America’s Most Convenient Bank,” is the tenth largest bank in the United States. Headquartered in Cherry Hill, New Jersey, the Bank has over 1,100 branches, or what TDBNA calls “stores,” along the eastern seaboard of the United States, including a large presence in New Jersey, New York, and Florida. Throughout the relevant period, as defined below, TDBNA’s retail banking activity involved providing banking products and services (e.g., checking and savings accounts, debit cards, and loans) to over 10 million individual and commercial customers in the United States.

2. TDBUSH, the direct parent of TDBNA, has oversight of the Bank's anti-money laundering ("AML") compliance program, including through reporting to TDBUSH's Audit Committee, and is accountable for monitoring the effectiveness of the Bank's AML program pursuant to the Bank Secrecy Act ("BSA"). TDBUSH in turn is the wholly owned subsidiary of TD Group US Holdings LLC ("TDGUS"), which is the intermediate holding company and ultimate parent holding company in the United States. TDGUS is responsible for oversight of the risk management framework for all U.S. operations, including AML programs. TDGUS is a wholly owned subsidiary of the Toronto-Dominion Bank d/b/a TD Bank Group, an international banking and financial services corporation located in Canada. TD Bank Group is the ultimate parent bank of all TD operations. Together, TDBNA, TDBUSH, TDGUS, and TD Bank Group, and their affiliates and subsidiaries, are referred to herein as TD or the Group.

3. Between January 2014 and October 2023 (the "relevant period"), TDBNA and TDBUSH failed to maintain an AML program that complied with the BSA and prioritized a "flat cost paradigm" across operations and the "customer experience." As a result, the Defendants willfully failed to remediate persistent, pervasive, and known deficiencies in its AML program, including (a) failing to substantively update its transaction monitoring system, which is used to detect illicit and suspicious transactions through the Bank, between 2014 and 2022 despite rapid growth in the volume and risks of the Bank's business and repeated warnings about the outdated system, and (b) failing to adequately train its employees who served as the first line of defense against money laundering. These failures enabled, among other things, three money laundering networks to launder over \$600 million in criminal proceeds through the Bank between 2019 and 2023. These failures also created vulnerabilities that allowed five Bank store employees to open and maintain accounts for one of the money laundering networks. These five Bank employees

ultimately conspired with criminal organizations to open and maintain accounts at the Bank that were used to launder \$39 million to Colombia.

4. TDBUSH's conduct, as described herein, constituted: (i) the willful failure to maintain an adequate AML program, in violation of Title 31, United States Code, Sections 5318(h) and 5322; and (ii) the knowing failure to accurately report currency transactions as required by the Secretary of the Treasury, in violation of Title 31, United States Code, Sections 5313 and 5324.

5. TDBNA's conduct, as described herein, constituted a conspiracy to: (1) willfully fail to maintain an appropriate AML program, contrary to Title 31, United States Code, Sections 5318(h), 5322; (2) knowingly fail to file accurate Currency Transaction Reports ("CTRs"), contrary to Title 31, United States Code, Sections 5313 and 5324; and (3) launder monetary instruments, contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i), all in violation of Title 18, United States Code, Section 371.

6. During the relevant period, Defendants willfully failed to maintain an adequate AML program at the Bank. At various times, high-level executives including those in Global AML Operations, in senior executive management, and on the TDBUSH Audit Committee—specifically including an individual who became Defendants' Chief Anti-Money Laundering Officer ("Chief AML Officer") during the relevant period (Individual-1) and the Bank's BSA Officer (Individual-2)—knew there were long-term, pervasive, and systemic deficiencies in the Defendants' U.S. AML policies, procedures, and controls. The Defendants did not substantively update the Bank's automated transaction monitoring system from at least 2014 through 2022—including to address known gaps and vulnerabilities in the TDBNA's transaction monitoring program—despite increases in the volume and risk of its business and significant changes in the nature and risk of transactional activity. In addition, during the relevant period, TDBNA monitored only

approximately 8% of the volume of transactions because it omitted all domestic automated clearinghouse (“ACH”) transactions, most check activity, and numerous other transaction types from its automated transaction monitoring system. Due to this failure, the Bank did not monitor approximately \$18.3 trillion in activity between January 1, 2018, through April 12, 2024. At the same time, Bank senior executives repeatedly prioritized the “customer experience” over AML compliance and enforced a budget mandate, referred to internally as a “flat cost paradigm,” that set expectations that all budgets, including the AML budget, would not increase year-over-year. The Defendants’ failures to appropriately fund the Bank’s AML program and to adapt its transaction monitoring program resulted in a willfully deficient AML program that allowed three money laundering networks to exploit the Bank and collectively transfer over \$670 million through TDBNA accounts. At least one scheme had the assistance of five store insiders at TDBNA.

7. From at least in or around January 2019 through in or around March 2021, the Defendants willfully failed to file accurate CTRs related to one of these three money laundering schemes. Da Ying Sze, a/k/a David (“David”), used TDBNA in furtherance of a money laundering and unlicensed money transmitting scheme for which he ultimately pled guilty in 2022. David conspired to launder and transmit over \$653 million, of which more than \$470 million was laundered through the Bank. David bribed Bank employees with more than \$57,000 in gift cards in furtherance of the scheme. David laundered money through the Bank by depositing large amounts of cash—occasionally in excess of one million dollars in a single day—into accounts opened by other individuals and by requesting that Bank employees send wires and issue official checks. TDBNA failed to identify David as the conductor of transactions in over 500 of the CTRs the Bank filed for his transactions, totaling over \$400 million in transaction value, despite David

entering TDBNA stores with nominee account holders and conducting transactions directly by making large cash deposits into accounts he purportedly did not control.

8. During the relevant period, TDBNA employed five individuals who provided material assistance, often in return for a fee, to a second money laundering scheme, which involved laundering tens of millions of dollars from the United States to Colombia. Insider-1 was a former Financial Service Representative at a TDBNA store in New Jersey. Insider-2 was a former Retail Banker at a TDBNA store in southern Florida. Insider-3 was a former Retail Banker at another TDBNA store in southern Florida. Insider-4 was a former Assistant Store Manager at a TDBNA store in eastern Florida. Insider-5 (jointly, the “TDBNA Insiders”) was a former Store Supervisor at another TDBNA store in southern Florida. These insiders opened accounts and provided dozens of ATM cards to the money laundering networks, which these networks used to launder funds from the United States to Colombia through high volume ATM withdrawals. The insiders assisted with maintaining accounts by issuing new ATM cards and resolving internal controls and roadblocks, including freezes on certain account activity. Through the accounts the insiders opened, the money laundering networks laundered approximately \$39 million through the Bank. Despite significant internal red flags, the Defendants did not identify the role the insiders played in the money laundering activity until law enforcement arrested Insider-1 in October 2023.

9. From March 2021 through March 2023, another money laundering organization that purported to be involved in the wholesale diamond, gold, and jewelry business (“MLO-1”) maintained accounts for at least five shell companies at TDBNA and used those accounts to move approximately \$123 million in illicit funds through the Bank. Since their account openings in 2021, TDBNA knew that these shell companies were connected because they shared the same account signatories. Despite these red flags, TDBNA did not file a Suspicious Activity Report (“SAR”) on

MLO-1 until law enforcement alerted TDBNA to MLO-1's conduct in April 2022. By that time, MLO-1's accounts had been open for over 13 months and had been used to transfer nearly \$120 million through TDBNA.

The Bank Secrecy Act and Other Relevant Legal Background

10. TDBNA is a national bank in the United States that is insured under the Federal Deposit Insurance Act and regulated and supervised by the Office of the Comptroller of the Currency ("OCC"). The Bank is therefore a financial institution for purposes of Title 31, United States Code, Section 5318(h).

11. The BSA, Title 31, United States Code, Section 5311, et seq., requires financial institutions—including TDBNA—to establish, implement, and maintain risk-based anti-money laundering programs to combat money laundering and the financing of terrorism through financial institutions.

12. The BSA requires that these AML programs, at a minimum, address five core pillars: (a) internal policies, procedures, and controls designed to guard against money laundering; (b) an individual or individuals responsible for overseeing day-to-day compliance with BSA and AML requirements; (c) an ongoing employee training program; (d) an independent audit function to test compliance programs; and (e) a risk-based approach for conducting ongoing customer due diligence. 31 U.S.C. § 5318(h); *see also* 31 C.F.R. § 1020.210.

13. To satisfy the BSA's requirements, a bank's AML program must be risk-based and its systems for identifying suspicious activity must be tailored to effectively monitor its customer-base and the products and services it offers, and reporting suspicious activity as required under the BSA. Moreover, a bank's AML policies, procedures, and controls must be calibrated to address

emerging and evolving risk, including risk associated with new products and services and new patterns of criminal activity.

14. For financial institutions of TDBNA's size and sophistication, an effective automated transaction monitoring system is necessary to properly identify, mitigate, and report suspicious activity as required by law and to prevent the institution from being used to facilitate criminal activity. Automated transaction monitoring systems filter transactions through a series of scenarios, or rules, in order to isolate a transaction or series of transactions with heightened indicia of money laundering, terrorist financing, or other illicit activity. If a transaction or series of transactions meet the parameters of a specific scenario, the automated transaction monitoring system generates an alert. Analysts then review each alert to determine whether the transaction was in fact suspicious and, if so, whether it should be escalated for further investigation or for the filing of a SAR with the United States Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), as required by the BSA. *See* 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320.

15. Under the BSA and its implementing regulations, financial institutions are also required to submit CTRs to FinCEN for "each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than \$10,000." 31 C.F.R. § 1010.311. Banks must file the CTR with FinCEN "within 15 days following the day on which the reportable transaction occurred," and must include "[a]ll information called for" in the "forms prescribed." 31 C.F.R. §§ 1010.306(a)(1), (a)(3), (d). The BSA describes CTRs as the types of "reports or records that are highly useful in . . . criminal . . . investigations," 31 U.S.C. § 5311, as they help establish a paper trail for law enforcement to identify large currency transactions, recreate financial transactions, and identify conductors and beneficiaries.

16. As part of the obligation to report currency transactions above \$10,000, a financial institution must “verify and record the name and address of the individual presenting a transaction, as well as record the identity, account number, and the social security or taxpayer identification number, if any, of any person or entity on whose behalf such transaction is to be effected.” 31 C.F.R. § 1010.312. Therefore, a bank is required to identify in its CTR filing the person who conducted the transaction (i.e., the conductor) in addition to the account holder. *See* 31 U.S.C. § 5313(a); FinCEN Form 104 (March 2011).

TDBNA and TDBUSH’s Failure to Maintain an Adequate AML Program

Background Regarding TDBNA’s BSA/AML Program

17. TD Bank Group is a publicly traded (NYSE: TD) international banking and financial services corporation headquartered in Toronto, Canada. TD Bank Group is one of the thirty largest banks in the world and the second-largest bank in Canada. TD Bank Group’s board is responsible for the supervision of the Group overall including major strategies, enterprise risk, executive hiring, and oversight of all subsidiaries. TD Bank Group’s board oversees and monitors the integrity and effectiveness of the Group’s internal controls and adherence to applicable compliance standards and is responsible for “setting the tone at the top as it relates to integrity and culture . . . and communicating and reinforcing the compliance culture throughout the [Group].”

18. TDGUS, incorporated in Delaware, is a wholly owned subsidiary of TD Bank Group. TDBUSH, which owns TDBNA, is a wholly owned subsidiary of TDGUS. Throughout the relevant period, TDBUSH and its Audit Committee oversaw TDBNA’s BSA/AML program, including issuing the BSA/AML Policy and Standards, approving the appointment of the BSA Officer, and receiving reporting and briefing on all AML program matters. According to TDBUSH’s BSA/AML Policy, “[t]he TDBUSH Board has ultimate responsibility for oversight of the [BSA/AML] Program and is accountable for monitoring its effectiveness regularly.”

TDBUSH's responsibilities included "[s]etting the 'tone from the top' commitment; and [p]articipating in briefings regarding inherent risks and controls, so that Board members attain an adequate level of understanding, as well as challenging the information presented to them about the [BSA/AML] Program matters."

19. During the relevant timeframe, TD Bank Group operated an AML program that applied across the global bank through the Global Anti-Money Laundering ("GAML") group. GAML established TD Bank Group's AML policies and procedures, decided issues related to AML budgeting and staffing Group-wide, and oversaw "shared services" groups that served both the U.S. and Canadian AML programs, including the AML technology team and AML Operations. GAML was led by the Chief AML Officer, to whom the BSA Officer and other senior AML executives reported. AML Operations, a group that served both U.S. and Canadian operations, encompassed both the U.S. and Canadian Financial Intelligence Units ("FIUs") at the Bank, which, among other critical functions, carried out the identification and reporting of suspicious activity. The head of the U.S. FIU had dual reporting lines to the BSA Officer and the Vice President, AML Operations, who, in turn, each reported directly to the Chief AML Officer. Therefore, some of TD Bank Group's AML functions were centralized and others were separated between the U.S. and Canada. (The U.S. AML program is referred to herein as "US-AML.")

20. During the relevant period, TDBNA had elements of an AML program that appeared adequate on paper. TDBNA had a BSA Officer who had relevant AML credentials; maintained policies and procedures targeting money laundering, terrorist financing, violations of U.S. sanctions, and other illicit activity; and implemented some controls necessary for the identification and reporting of suspicious activity. Despite these efforts, however, there were

fundamental, pervasive flaws in the Bank's transaction monitoring program, which created an environment that allowed financial crime to flourish.

21. Individual-1, whose identity is known to the Offices and Defendants, was the Group's senior AML executive during all of the relevant period. TDBNA hired Individual-1 in 2013 as the VP, AML Operations, reporting directly to the then Chief AML Officer. In approximately 2017, Individual-1 was promoted to Co-Head of Global AML and thereafter effectively shared the Chief AML Officer responsibilities with another individual. In early 2019, Individual-1 became the sole Chief AML Officer, a position he held until 2023. As both the Co-Head of GAML and the Chief AML Officer, Individual-1 was responsible for TD's Group-wide AML program, which included establishing the annual Group-wide AML budget, setting GAML priorities, spearheading GAML's strategic planning, and regularly briefing the TD Bank Group and TDBNA boards of directors on AML compliance matters. Individual-1, as Chief AML Officer, also had specific oversight responsibilities related to US-AML, including oversight of TDBNA's BSA Officer; oversight of AML technology services, which was shared between the U.S. and Canada; and shared oversight, with the BSA Officer, of the U.S. FIU.

22. Individual-2, whose identity is known to the Offices and the Defendants, was an AML executive at TDBNA for nearly the entire relevant period. Individual-2 joined TDBNA in 2014 as Head of the U.S. FIU and, in that role, supervised the investigative teams responsible for reporting suspicious activity, filing CTRs, managing high-risk customers, and preventing sanctioned transactions. In January 2018, Individual-2 was promoted to Deputy BSA Officer and, in May 2019, assumed the roles of BSA Officer and Deputy Global Head of AML Compliance, which Individual-2 held until May 16, 2023. As BSA Officer, Individual-2 was responsible for US-AML, including establishing the budget and managing staffing, assessing the Bank's AML

risk, approving policies and procedures, and presenting to the TDGUS and TDBUSH boards of directors. In practice, Individual-2 was required to obtain approval from the Chief AML Officer, Individual-1, for the US-AML annual budget, as well as for all hiring decisions. Because the AML technology group reported directly to the Chief AML Officer, Individual-2 believed that issues related to US-AML technology were outside of Individual-2's supervision.

23. From 2016 through 2022, Individual-3, whose identity is known to the Offices and the Defendants, was a vice president and senior manager within AML Operations for TDBNA. Individual-3 also informally served as Head of the U.S. FIU from in or around 2017, when Individual-2 left that role, until a replacement was hired in or around December 2018. In AML Operations, Individual-3 oversaw various components of the U.S. FIU's AML functions, including the teams tasked with the initial review of transaction monitoring alerts and with managing Unusual Transaction Referrals ("UTRs"), which were reports of potentially suspicious conduct submitted by employees through TDBNA's internal reporting system.

Transaction Monitoring Issues Were Repeatedly Identified to TDBNA

24. Over at least the past eleven years, the OCC, FinCEN, TDBNA Internal Audit, and third-party consultants have repeatedly identified TDBNA's transaction monitoring program as an area of concern. The senior executive leadership and boards of directors of TDBNA, TDBUSH, TDGUS, and TD Bank Group were made aware of certain of the concerns identified by these regulators and auditors.

25. On September 23, 2013, the OCC and FinCEN announced enforcement actions against TDBNA carrying a combined civil monetary penalty of \$37.5 million for violations of the BSA stemming from a Ponzi scheme orchestrated by a Florida attorney. TDBNA's board and the then-head of TDBNA signed the 2013 OCC Agreement. Despite the numerous AML alerts generated by its transaction monitoring program, TDBNA failed to timely identify and report

approximately \$900 million in suspicious activity related to the scheme. According to FinCEN, TDBNA's failures were due, in part, to inadequate AML training for both AML and retail personnel. In announcing the resolution, the FinCEN Director noted, "[i]t is not acceptable to have a poorly resourced and trained staff overseeing such a critical function."

26. TDBNA failed to effectively or substantively adapt its transaction monitoring system after the 2013 enforcement actions. For example, in 2013, the OCC determined that TDBNA needed to develop transaction monitoring policies and procedures to ensure systematic and prompt responses to environmental or market-based changes, i.e., policies and procedures concerning the development of new transaction monitoring scenarios or manual processes to appropriately mitigate emerging risks. In 2018, the OCC characterized TDBNA's planning, delivery, and execution of AML technology systems and solutions as insufficient. Specifically, the OCC highlighted the delays in implementing multiple AML technology projects and found those delays to be directly linked to nearly all of TDBNA's outstanding AML program issues.

27. In 2018, TDBNA Internal Audit, which periodically assessed the Bank's AML program and specific functions within US-AML, determined that TDBNA's high-risk jurisdiction transaction monitoring scenarios were using an outdated list of high-risk jurisdictions, meaning the bank's scenarios were not designed to generate alerts on the jurisdictions currently deemed to be high risk. In 2020, TDBNA Internal Audit identified AML compliance deficiencies related to the governance and review of transaction monitoring scenarios, including that: (i) TDBNA lacked formal timelines for completing its scenario reviews, many of which had remained outstanding since 2017; (ii) TDBNA had not implemented its proposed changes to U.S. scenarios from the previous year; and (iii) TDBNA had no "procedure or formal document outlining the process to follow nor factors/trigger points for the promotion of new scenarios in [the transaction monitoring

system] or in a manual environment.” The third finding, regarding the lack of governance of transaction monitoring scenario development, involved the same issues as the OCC finding from seven years earlier. All of these findings remained unresolved during the following year’s TDBNA Internal Audit review. The Defendants’ boards were informed of Internal Audit findings and associated remediation plans.

28. During the relevant period, TDBNA also engaged third-party consultants who identified fundamental weaknesses in the Bank’s AML program, which were reported to GAML leadership. For example, in 2018, one consultant commented that “increased volumes and regulatory requirements” would put pressure on AML operations to meet demands and deadlines. The same consultant concluded that the Bank’s required testing of its transaction monitoring scenarios—which assessed whether scenarios were adequately capturing suspicious activity—took twice as long as the industry average. In 2019, another consultant found that TDBNA had “sub-optimal [transaction monitoring] scenarios” due, in part, to “outdated parameters” that generated a large volume of alerts that limited “GAML’s ability to focus on high risk customers and transactions.” In 2021, a third consultant identified numerous limitations in the Bank’s transaction monitoring program, including technology barriers to developing new scenarios or adding new parameters to existing scenarios.

TDBNA Failed to Update its Transaction Monitoring Program, Despite Known Gaps, Leaving Trillions of Dollars of Customer Activity Entirely Unmonitored

29. An effective AML transaction monitoring program must be capable of adapting to changes in the banking industry, including new methods of money laundering and new banking products and services. Indeed, in September 2021, Individual-2 informed the boards of directors for TD Bank Group, TDGUS, and TDBUSH that, “included within GAML’s responsibilities is to

have an appropriate framework in place to identify and monitor both emerging and evolving risk.” Yet over the relevant period, the Bank did not adapt its transaction monitoring system.

30. Throughout the relevant period, TDBNA utilized an automated transaction monitoring system to detect and generate alerts on suspicious transactions and activities. From at least 2014 to late 2022, TDBNA failed to implement any new transaction monitoring scenarios or make any substantive changes to the parameters of its existing transaction monitoring scenarios, despite significant unaddressed risks. For example, TDBNA did not have any scenarios to monitor changes and anomalies in a particular customer’s transaction behavior, a standard indicator of suspicious activity, or any specific scenarios to monitor customers it deemed to be higher risk, such as money services businesses and precious metals dealers. And although TDBNA typically applied different dollar scenario thresholds to personal accounts and business accounts, the Bank did not apply different standards to different business accounts, meaning that a Fortune 500 company was subject to the same scenarios and dollar thresholds as a sole proprietorship, despite fundamental differences in the type and volume of activity.

31. These transaction monitoring deficiencies were exacerbated by TDBNA’s failure to implement any new scenarios or materially modify any existing scenarios during the relevant period. As acknowledged in TDBNA’s draft document titled, *New Transaction Monitoring Scenario Development Procedures (2017)*, which was never finalized, “[a] new transaction monitoring scenario may be required . . . if [an] existing transaction monitoring scenario does not cover the intended risk.”

32. During the relevant period, US-AML employees escalated known gaps in the Bank’s transaction monitoring system to GAML and US-AML management and proposed new or enhanced scenarios to address those risks. Individual-1 pointed to TDBNA’s legacy technology

systems as a contributor to TDBNA's failure to implement or modify any scenarios. However, TDBNA not only failed to implement any automated solutions, it also did not create any effective manual transaction monitoring solutions or employ other stopgap measures until it could implement a more permanent solution.

33. Beginning as early as 2008, TDBNA severely limited the types of activity it screened through its transaction monitoring system. Specifically, after approximately 2011, TDBNA did not monitor *any* domestic ACH activity, most check activity, internal transfers between accounts at TDBNA, or numerous other transaction types. This decision had a profound effect on TDBNA's ability to monitor and report suspicious activity, as required by the BSA. As a result of this decision, between January 1, 2018, and April 12, 2024, TDBNA's automated AML monitoring failed to monitor 92% of transaction volume and 74% of transaction value, which corresponded to over 14.6 billion unmonitored transactions and over \$18.3 trillion in unmonitored transaction value, which included a mix of lower- and higher-risk transactions.

34. Since 2008, TDBNA did not conduct any systematic analysis to review decisions not to monitor certain transaction types or whether they continued to be appropriate over the course of more than a decade. US-AML employees *did* repeatedly propose automated monitoring solutions to mid-level AML leadership to close this substantial gap. In 2012, after conducting a risk assessment, TDBNA elevated the AML risk of domestic ACH to "medium," largely due to the lack of monitoring, and this elevated rating remained in place during the entirety of the relevant period. In response, US-AML personnel proposed adding transaction monitoring scenarios to identify potentially suspicious domestic ACH activity. A GAML executive rejected this proposal. In 2019 and again in 2020, another US-AML employee highlighted the lack of domestic ACH and check monitoring to mid-level US-AML supervisors and unsuccessfully advocated for the

implementation of automated solutions. Throughout this period, certain individuals within GAML and US-AML including senior leadership, were aware of the lack of domestic ACH and check monitoring.

35. During the relevant period, while allowing the majority of its customers' activity to go unmonitored, TDBNA introduced new products and services and failed to address the AML risks associated with those products with any new or enhanced transaction monitoring scenarios.

a. In April 2017, for example, TDBNA began offering its individual customers access to Zelle, a mobile, person-to-person payment platform that allows its users to transfer funds between accounts at participating financial institutions. During the relevant period, TDBNA individual customers transferred over \$75 billion in Zelle transactions, which was almost entirely unmonitored.

b. Although US-AML employees began assessing the money laundering risk associated with Zelle before its implementation, TDBNA failed to screen any Zelle activity through its transaction monitoring system until March 2020. In August 2020, TDBNA incorporated Zelle activity into two existing transaction monitoring scenarios covering suspicious wire activity in personal accounts but failed to recalibrate the scenarios to effectively identify suspicious Zelle activity, which typically involved lower transaction values and higher volumes than suspicious wire activity. In fact, those two scenarios only flagged personal customer activity exceeding \$10,000 in deposits or \$9,000 in transfers over a 5-day period, yet personal Zelle activity was capped at \$10,000 during a rolling 30-day period. In other words, the scenarios captured activity that effectively could not occur through Zelle.

36. In July 2021, US-AML executives told the OCC during its annual examination that the Bank was conducting "scenario based monitoring" of Zelle activity based on the two scenarios

to which Zelle had been added. US-AML employees continued to identify Zelle as a gap in TDBNA's transaction monitoring program, with one employee noting that, "because we haven't been able to write a net new scenario," suspicious Zelle activity "gets lost in the much bigger \$ wire category." Several US-AML employees continued to advocate to mid-level management for the implementation of appropriately calibrated scenarios to alert on suspicious Zelle activity, but GAML put the Zelle scenario project on hold in late 2021 because it was not "an exposed risk or regulatory need."

37. In 2015, the OCC instructed TDBNA to enhance its transaction monitoring program for high-risk customers, which were subject to the same scenarios and thresholds as the rest of TDBNA's customers despite their higher risk profile. In 2016, as part of that effort, the US-AML, GAML, and TD Bank Group technology teams began to develop new high-risk customer scenarios. That effort was put on hold in October 2016 by GAML executives due to a lack of resources. After being briefly revived in early 2017, this project was again put on hold, this time by Individual-1, partly due to "cost." Although US-AML leadership informed the OCC during its examinations in 2017, 2018, and 2019 that these scenarios were in development, TDBNA never implemented the required enhanced transaction monitoring of high-risk customers.

38. TDBNA left other significant gaps in its transaction monitoring program. For example, in or around 2011, TDBNA decommissioned several scenarios targeting large cash activity by businesses and other non-personal customers with the stated intention to test and recalibrate the scenario thresholds, identify potentially new parameters, and redeploy the scenarios. But the Bank did not do this. In fact, these scenarios remained offline from 2011 until late 2022, which allowed suspicious cash activity to be processed without alerts, including

hundreds of millions of dollars of transactions by two of the money laundering networks detailed below.

39. The limited changes TDBNA made to its scenarios during the relevant period almost exclusively—and intentionally—reduced the universe of alerts being generated and thereby lowered the associated cost of their review. Indeed, while TDBNA did not add any new transaction monitoring scenarios during the relevant period, it removed at least nine.

40. In February 2018, another U.S. bank entered into a negotiated resolution with the Department of Justice for its programmatic AML failures and failure to file SARs, the former of which was predicated, in part, on the bank's cessation of transaction monitoring scenario threshold testing. Senior US-AML executives were aware of this resolution and understood that banks must monitor their transactions for suspicious activity, with Individual-2 explaining to the AML Oversight Committee that "We always look at one of these actions and look at our own program and compare the conduct that has occurred. We look at our own processes to make sure nothing like this is happening. . . ." Specific to scenario threshold testing, Individual-2 asserted that "for each one of our scenarios we will do a lot of analysis and work below each threshold to see if SARs should have been filed. If we are seeing a certain percentage of SARs that would be filed, then we will look at whether we would lower that threshold on that particular scenario. ... In contrast, [the U.S. bank] either ignored or discontinued that below the line threshold testing." Nevertheless, by the beginning of 2018, US-AML, along with its GAML technology partners, effectively stopped conducting threshold testing on its scenarios due to competing priorities and limited resources. As a result, from 2018 through 2022, TDBNA conducted threshold testing—what it referred to as "quantitative tuning"—on only one of its approximately 40 U.S. transaction monitoring scenarios.

41. In another example, throughout the relevant period, TDBNA maintained and regularly updated a list of “high-risk countries,” which were jurisdictions found to have higher indicia of risk, including AML and terrorist financing risk. US-AML, however, only effectively monitored transactions involving what it dubbed “high high risk countries” (“HHRCs”), which were a subset of the high-risk country list and which were not updated after 2013, regardless of any changes to TDBNA’s high-risk country list, updates to the Financial Action Task Force’s¹ “grey list,” or other geopolitical events. During this same period, GAML executives removed numerous countries from the HHRC transaction monitoring scenarios and only approved threshold changes that “would have no impact or lower the volume of false positives.” In other words, GAML prioritized reducing alerts and the associated cost savings over identifying suspicious activity involving high-risk countries. Until at least December 2023, countries like the Dominican Republic and Jamaica were not included on the HHRC list, even though US-AML employees repeatedly identified suspicious ATM activity involving such countries.

GAML Operated under Budget Constraints

42. GAML’s budget was a primary driver of its decisions about projects, hiring, staffing, and technology enhancements throughout the relevant period. GAML executives strove to maintain what TD Bank Group referred to as a “flat cost paradigm” or “zero expense growth paradigm,” meaning that each department’s budget, including GAML’s, was expected to remain flat year-over-year, despite consistent growth in TD Bank Group’s revenue over the relevant

¹ The Financial Action Task Force (“FATF”) is an international policy-making and standard-setting body charged with safeguarding the global financial system from money laundering and terrorist financing. The “grey list” identifies countries that FATF determined to have strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing.

period. This budgetary pressure originated with senior bank executives and was achieved within GAML and US-AML by Individual-1 and Individual-2, both of whom touted their abilities to operate within the “flat cost paradigm without compromising risk appetite” in their self-assessments. GAML’s base and project expenditures on US-AML were less in fiscal year 2021 than they were in fiscal year 2018 and were not sufficient to address AML deficiencies including substantial backlogs of alerts across multiple workstreams, despite TDBNA’s profits increasing approximately 26% during the same period. In 2019, Individual-1 referred to the Bank’s “historical underspend” on compliance in an email to the Group senior executive responsible for the enterprise AML budget, yet the US-AML budget essentially stayed flat. GAML and US-AML employees explained to the Offices that budgetary restrictions led to systemic deficiencies in the Bank’s transaction monitoring program and exposed the Bank to potential legal and regulatory consequences.

43. At certain points throughout the relevant period, TDBNA postponed or cancelled proposed improvements to its transaction monitoring program, often to reduce AML costs. For instance, in August 2019, several US-AML and GAML executives, including Individual-2, met to discuss the fiscal year 2020 budget and identified several transaction monitoring projects to postpone, referring to them as “opportunities to reduce expenses for 2020/Opportunity to push out to future years.” The group postponed a project designed to “Enhance Functionality and Scenario Development for U.S.” because “new scenario development means new data and a lot of work effort.” The group also postponed a project related to “Manual Monitoring,” finding that it would require “new data feeds” and “scenarios” and there was “no capacity to do this.” The Bank never completed either of these postponed projects.

Bank Employees Openly Discussed the Bank's Facilitation of Criminal Activity

44. TDBNA's failures to address emerging risks and new products and its focus on operational risk versus programmatic risk resulted in employees throughout the Bank discussing the efficacy of TDBNA's AML program. In October 2021, when asked by a colleague what "the bad guys" thought about the Bank's AML program, GAML's lead AML technologist and one of Individual-1's direct reports summarized the program as follows:

AML Technologist	what do the bad guys have to say about us
GAML Manager	Lol
GAML Manager	Easy target
AML Technologist	damnit
GAML Manager	Old scenarios ; old CRR ; tech agility is poor to react to changers
GAML Manager	Bottomline we have not had a single new scenario added since we first implemented SAS due to various issues with the install

45. Other employees, both in GAML and retail, consistently commented on the Bank's instant messaging platform about the Bank's motto, "America's Most Convenient Bank," and directly linked it to the Bank's approach to AML. For example, a US-AML employee noted that a reason the Bank had not stopped one of the below-referenced money laundering typologies was because "we r the most convenient bank lol." Similarly, when two US-AML employees discussed another one of the below-referenced money laundering typologies, as well as other customers engaged in potentially suspicious activity, the following conversation occurred:

Employee 1	:P why all the really awful ones bank here lol
Employee 2	because...
Employee 2	we are convenient

Employee 2 hahah

Employee 1 bahahahahaha

Employee 1 that was their worst move evvvver

46. Others discussed cost and other impediments associated with developing new scenarios. For example, in both 2018 and 2020, an AML technologist sought to initiate scenario development projects, but both were ultimately deemed to be out of scope, decisions the AML technologist attributed directly to budgetary limitations. Also in 2020, a US-AML employee, in discussing an unfulfilled automated solution to an existing manual process, noted that GAML “can not properly code the scenario to give us what we want and its [sic] too much money to hire a coder Lol[.]”

TDBNA’s AML Failures Allowed Millions In Illicit Funds To Flow Through the Bank

47. Multiple money laundering networks took advantage of TDBNA’s deficient AML program and permissive procedures to launder at least \$671 million in suspected illicit proceeds through TDBNA accounts.

48. Between January 2018 and February 2021, Da Ying Sze, who was known to TDBNA employees as “David,” and his co-conspirators (collectively, “David’s Network”) moved approximately \$474 million through TDBNA stores in New Jersey, New York, Pennsylvania, Maine, and Florida. According to David, who attempted to launder money through numerous financial institutions, TDBNA had by far the most permissive policies and procedures. As a result, TDBNA was where David chose to launder most of his funds. In February 2022, David pleaded guilty to engaging in more than \$653 million in monetary transactions in property derived from a specified unlawful activity, operating an unlicensed money transmitting business, and bribing bank

employees. Four of David's co-conspirators similarly pleaded guilty to unlicensed money transmitting charges.

49. In furtherance of his scheme, David used nominees to set up shell companies and opened bank accounts in the names of those nominees and shell companies at TDBNA, or to use existing accounts that had previously operated without suspicious activity. David then laundered bulk cash through these TDBNA accounts, depositing up to millions of dollars of cash in a single day; immediately moved the funds out of the accounts using official bank checks and wire transfers; and conducted other transactions despite being neither an accountholder nor a signatory. David's Network also moved a substantial amount of illicit funds through TDBNA personal accounts, and in some instances David told TDBNA employees that he was using the personal accounts for business transactions because they incurred fewer bank fees. Throughout his money laundering scheme at TDBNA, David distributed over \$57,000 in retail gift cards to TDBNA retail employees. According to David, the gift cards were meant to ensure that Bank employees would continue processing his transactions.

50. David's suspicious activity was obvious even to the casual observer. For example, the surveillance photograph below depicts David conducting a \$372,000 cash transaction at a midtown New York store on July 21, 2020. David transacted in accounts that were not in his name. As depicted below, an account holder sat in the background not participating in the transaction while David, who was not the account holder, conducted the transaction. The account owner's lack of participation makes clear that while the account was opened in someone else's name, David actually controlled the account. That same day, David conducted a \$290,000 cash transaction at a different TDBNA store. During these transactions, David purchased 14 official bank checks.



51. Throughout 2020, Individual-2 regularly received reports that aggregated and analyzed the Bank's CTR and monetary instrument activity. Within those reports, the extraordinary volume and value of David's Network's official bank check activity were repeatedly highlighted as substantial outliers. The February 2020 report called out two of the companies in David's Network for purchasing a total of \$8.5 million in official bank checks, the highest amount of official bank checks at two different TDBNA stores. The report further noted that \$8.3 million of those official bank checks were purchased with cash. Business and personal accounts linked to David's Network (but not held by David himself) were singled out in subsequent reports to Individual-2 throughout 2020 for outlier activity. Individual-2 stated that she did not review the reporting carefully because she incorrectly assumed that other US-AML executives were also receiving the reports, although she was the sole recipient. As a result, these reports did not initiate any additional investigation concerning David's Network.

52. TDBNA Retail employees at multiple levels understood and acknowledged the likely illegality of David's activity. In August 2020, one TDBNA store manager emailed another store manager and remarked, "You guys really need to shut this down LOL." In late 2020, another store manager implored his supervisors (several TDBNA regional managers) to act, noting that "[i]t is getting out of hand and my tellers are at the point that they don't feel comfortable handling these transactions." In February 2021, one TDBNA store employee saw that David's Network had purchased more than \$1 million in official bank checks with cash in a single day and asked, "How is that not money laundering," to which a back-office employee responded, "oh it 100% is."

53. Retail employees also alerted US-AML personnel to David's suspicious activity through their submission of UTRs, which were the primary means for TDBNA retail employees to escalate potentially suspicious behavior to TDBNA's Financial Intelligence Unit, which assessed the UTR and fed it into the suspicious activity review stream, the primary means by which US-AML could be alerted to suspicious in-store conduct. Per TDBNA policy, employees that "identify an unusual activity or transaction or potentially suspicious conduct . . . must escalate or report it in accordance with [their] Business Unit procedures" through the submission of a UTR. Without retail employee submission of UTRs, it would be difficult for US-AML to know, for example, that a customer refused to provide identification during an in-store transaction or, as with David's Network, that a third party was regularly conducting transactions in multiple accounts that were not in their name.

54. For David's Network, the suspicious activity far outpaced the number of UTRs filed. Retail employees repeatedly failed to report David's suspicious transactions, including the deposit pictured above in paragraph 50. In the UTRs employees did file, the retail employees clearly communicated the gravity of the conduct. In a UTR from January 5, 2020, a retail employee

wrote that the activity “might be part of group that has been depositing extremely large amount of cash and possible laundering money.” On September 9, 2020, a different retail employee succinctly reported to US-AML that, “EVERY DAY CUSTOMER DEPOSIT A LOT OF CASH.” In another UTR from November 2020, a retail employee reported to GAML that they did “not feel comfortable doing their deposits knowing the activity is highly suspicious.”²

55. The US-AML employees tasked with UTR intake and escalation were aware of David’s Network, with one noting in July 2020 that “[t]hey have certainly been a thorn in our side for quite some time!!” The UTR team was regularly understaffed—in part due to the Bank’s “flat-cost paradigm”—and the intake process was manual and laborious, which frequently resulted in backlogs. As a result, US-AML’s UTR team tried to reduce the number of incoming UTRs, particularly on repeat subjects like David’s Network that had already generated alerts. In August 2020, Individual-3 approved an updated procedure that allowed the UTR intake team to inform stores that additional UTRs were not required on specific customers unless the customers’ unusual activity changed or continued beyond 60 days. This procedural change, which directly contravened TDBNA policies, resulted in multiple TDBNA stores being informed that no further UTRs were necessary on specific customers, including David’s Network. Upon receipt of this guidance from US-AML, several retail employees assumed this instruction indicated that the activity was within the Bank’s risk tolerance.

56. The limited universe of UTRs was exacerbated by the inaccurate CTRs the Bank submitted for activity involving David’s Network, which almost uniformly failed to identify David as the conductor of the transactions. Consistent with the BSA, TDBNA policy required store

² Based on the UTRs from retail employees and the transaction monitoring alerts, the Bank eventually filed SARs on David’s Network. These SARs failed to include David and only involved approximately 70% of the suspicious activity related to David’s Network.

employees to collect information from the “person conducting transaction for another” and in training materials advised employees to identify the “conductor” in CTRs, i.e., “the person(s) who physically conducts the transaction.” In practice, however, employees regularly identified only the TDBNA accountholder on the CTR form, which TDBNA enabled by prepopulating the accountholder information on the CTR form. For example, in the surveillance photo in paragraph 50, above, the corresponding CTR listed the TDBNA customers—including the shell companies, and their individual nominee owners who held the accounts on behalf of David—as the “person conducting transaction on own behalf,” not David, the obvious conductor of the transaction.

57. This was not an isolated failure. TDBNA’s CTR failures spanned numerous stores and dozens of employees. Of the hundreds of CTRs filed on activity in accounts linked to David’s Network, indicia of David’s involvement were included on only 20 CTRs. As a result, TDBNA willfully filed 564 materially inaccurate CTRs that did not identify David as the conductor of the transaction. These materially inaccurate CTRs, which spanned from June 2019 through February 2021 and covered transactions totaling \$412,876,589, subverted the purpose of the CTR form and impeded law enforcement’s ability to identify and prevent money laundering.

58. In addition, from March 2021 through March 2023, MLO-1 maintained accounts for at least five shell companies at TDBNA and used those accounts to move approximately \$123 million in illicit funds through the Bank. Since their account-openings in 2021, TDBNA knew that these shell companies were connected because they shared the same account signatories. Retail employees submitted two UTRs highlighting the suspicious nature of MLO-1’s activity, including that the cash deposits were “excessive for their type of industry.” Despite these red flags, TDBNA did not file a SAR on MLO-1 until law enforcement alerted TDBNA to MLO-1’s conduct in April

2022. By that time, MLO-1's accounts had been open for over 13 months and had been used to transfer nearly \$120 million through TDBNA.

59. TDBNA's failure to file SARs on MLO-1 in a timely manner is attributable to the Bank's transaction monitoring failures. First, TDBNA's transaction monitoring system did not generate a single automated alert on MLO-1's primary deposit account (the "Management Account"), where the MLO deposited over \$122 million in cash. By 2021, when MLO-1 first began to transact through TDBNA, TDBNA had long decommissioned its transaction monitoring scenario targeting large-cash deposits by business customers, as detailed above. Had this decommissioned scenario been active during the 13 months of MLO-1's activity, it would have generated approximately 161 transaction monitoring alerts on MLO-1's Management Account over the course of the \$122 million in deposits.³

60. Second, TDBNA's transaction monitoring scenarios targeting "high-velocity" transactions (where the money moves out quickly after deposit) failed to monitor most transaction types, including the intrabank transfers utilized by MLO-1. Therefore, immediately after depositing a large sum of cash into the Management Account, MLO-1 was able to quickly transfer the funds to its other accounts at TDBNA without detection. This type of high-velocity transaction is a common indicator of money laundering. In mid-2019, a GAML employee identified this monitoring gap for high-velocity transfers, noting, "it does not appear there are scenarios focused on expedient money movement across all TD products." Although a remedial scenario was added to a scenario development list in early 2020, no such scenario was ever developed. Accordingly,

³ The same transaction monitoring scenario, had it been operational, would have generated an additional 271 alerts on business accounts controlled by David's Network.

none of the high-velocity transfers from the Management Account to MLO-1's other TDBNA accounts, totaling approximately \$120 million, generated an alert.

61. Third, while TDBNA identified the MLO-1 accounts as high-risk because they were allegedly involved in the precious metals business, TDBNA employed no enhanced transaction monitoring scenarios to identify suspicious conduct by such high-risk entities, although the accounts were subject to periodic reviews. This gap caused US-AML to receive fewer alerts than were warranted, given the highly suspicious nature of MLO-1's profile.

62. Additionally, beginning no later than 2018 and continuing through October 2023, TDBNA failed adequately to thwart a method of money laundering involving depositing funds into personal and business accounts in the United States and withdrawing cash at ATMs in Colombia (the "Colombian ATM Typology"). The Colombian ATM Typology, which FinCEN has designated as a risk for the financial industry,⁴ persisted at TDBNA in part due to considerations that account restrictions could impair the customer experience and the Bank's failure to implement controls and procedures to enforce its AML policies. For example, TDBNA failed to implement appropriate internal controls to enforce its fifteen-debit card limit per business account and its requirement that customers be present during account opening and debit card issuance, which allowed insiders to provide dozens of ATM cards to money laundering networks. Further, TDBNA's fee structure for certain account types allowed money launderers to withdraw cash at Colombian ATMs without incurring any bank fees. As discussed below, the Colombian ATM Typology was also aided by the TDBNA Insiders.

⁴ See, e.g., FinCEN Advisory, *Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering*, FIN-2010-A001 (Feb. 19, 2010).

63. Between November 2019 and November 2022, a money laundering network (“MLO-2”) used TDBNA to transfer over \$39 million in illicit funds using the Colombian ATM Typology. In furtherance of this scheme, MLO-2 aggregated funds into bank accounts at various financial institutions, wired the funds to one of its approximately thirty TDBNA checking accounts, and then immediately withdrew the funds at ATMs in Colombia using debit cards. To facilitate these withdrawals, MLO-2 took advantage of TDBNA’s deficient AML controls and paid kickbacks to an insider to obtain as many TDBNA debit cards as possible.

64. TDBNA accounts were particularly conducive to MLO-2’s scheme for several reasons. First, some TDBNA stores did not enforce the requirement for debit card signatories to appear in person and instead allowed MLO-2 to present screenshots or photocopies of Venezuelan passports as identification. MLO-2 also reused the same Venezuelan passports across their TDBNA bank accounts, and sometimes used the same passport to obtain multiple debit cards for a single account. In some instances, representatives of MLO-2 were not required to provide any identification to obtain debit cards. Second, TDBNA would issue as many debit cards as MLO-2 requested for its business checking accounts, despite an internal policy establishing a 15-card limit per account. This allowed MLO-2 to obtain, in certain cases, up to 46 debit cards per TDBNA account and move money to Colombia in amounts 40 to 50 times higher than the daily withdrawal limit for personal accounts. Third, TDBNA’s favorable fee structure for foreign ATM withdrawals as compared to its peer banks resulted in lower bank fees for MLO-2. As a result, approximately 70% of the total funds MLO-2 moved to Colombia were withdrawn using TDBNA accounts. An effective and properly resourced AML program would have identified and appropriately mitigated these risks.

65. MLO-2 was one of several money laundering organizations exploiting TDBNA accounts to move millions of dollars to Colombia. Some of this money laundering activity was facilitated by the TDBNA Insiders, who were responsible for opening accounts that transferred over \$39 million to Colombia through a total of 194,940 ATM withdrawals.

66. TDBNA's failure to effectively manage its employee risk contributed to this insider misconduct—a result that was reasonably foreseeable to GAML and US-AML leadership in light of TDBNA's pervasive AML failures. The TDBNA Insiders opened personal and business accounts for individuals engaged in the Colombian ATM Typology, including MLO-2,⁵ in exchange for bribes ranging from \$50 to \$2,500 per account. Insider-2 and others received these bribes directly into their personal accounts at TDBNA via Zelle—including some Zelle transfers directly from the TDBNA accounts the insider had opened. Insider-1 even used several of the illicit debit cards they issued to withdraw money directly from an ATM in their own TDBNA store.

67. In exchange for these bribes, the TDBNA Insiders opened accounts in the names of shell companies and nominee owners, often without the accountholder present; corresponded with the money launderers during the account's lifespan, often using their TDBNA email addresses; resolved any issues that arose while the accounts were active, including unblocking and replacing debit cards; and assisted with opening new accounts if and when an existing account was closed. For business accounts, the TDBNA Insiders were able to issue numerous debit cards—in some instances more than 50—for a single account, in contravention of TDBNA policy.

68. Despite numerous red flags, which the Bank did not appropriately act on, the Bank did not identify the TDBNA Insiders' misconduct, sometimes for years, until law enforcement intervention in late October 2023. For example, Insider-1, from a TDBNA store in New Jersey,

⁵ Both Insider-1 and Insider-5 opened accounts for MLO-2.

opened numerous accounts for businesses with addresses listed in Florida. After Insider-1 was arrested by law enforcement, the Bank helped law enforcement identify similar misconduct by the additional insiders. Insider-2 opened dozens of accounts in the names of foreign citizens using a single address in Miami, Florida. Insider-3 issued dozens of debit cards to a number of business accounts and openly scheduled in-store pickups and other logistics with his TDBNA email address. Insider-4, after receiving text messages with personal information and corresponding Zelle payments, opened over one hundred accounts for individuals that were not present at account opening, including opening an account when the store was closed. Insider-5, who was linked to the Colombian ATM Typology during two different stints working at TDBNA, also opened accounts for individuals who were not present at account opening. Several of the TDBNA Insiders personally completed and signed tax documents and other account opening forms in furtherance of their misconduct.

69. In or around April 2019, TDBNA became aware of the Colombian ATM Typology, after the newly created Business Intelligence team within US-AML analyzed a series of accounts being used to funnel money to Colombia. This analysis explicitly likened the Colombian ATM activity to the FinCEN advisory noted above and identified patterns in the timing and location of the activity, including stores where the activity was most prevalent.⁶ The analysis also revealed that certain accounts engaged in this activity were opened on the same day and using the same address. Business Intelligence provided a series of recommendations and next steps for addressing the Colombian ATM Typology, including that TDBNA: (i) engage in store-level training specific to the activity; (ii) investigate “inside jobs/involvements”; (iii) identify any similar accounts

⁶ The list of stores Business Intelligence identified included the stores where Insider-3 and Insider-5 eventually worked.

beyond the 74 included in the initial analysis; and (iv) reconsider specific policies and procedures related to account openings and third-party cash deposits.

70. A version of this analysis was shared with the highest levels of GAML and US-AML, including Individual-2. On July 29, 2019, Individual-2 received this analysis and the proposed recommendations. In September 2019, a similar presentation was provided to the GAML Senior Executive Team, which was led by Individual-1 and included Individual-2. The same month, several mid-level US-AML executives convened to discuss the Colombian ATM Typology, during which they acknowledged that peer banks had instituted policies and safeguards that were closing the bad actors out of these banks and resulting in them seeking to use TDBNA, and agreed that the only way to prevent TDBNA from being used for this type of money laundering was for US-AML to influence retail policy change.

71. Yet, over the next eighteen months, TDBNA did not enact any of the changes or recommendations identified in Business Intelligence's analysis to address the Colombian ATM Typology. Although US-AML, including Individual-2 and their direct reports, discussed potential changes to retail policies and procedures with business-side personnel, such changes were ultimately abandoned due to the potential impact on the "customer experience" and the associated increased staffing requirements. Beginning in July 2020, in response to the Colombian ATM Typology, US-AML personnel sought to create an AML monitoring framework for business accounts with a high number of associated debit cards, but no such framework was implemented. During this period, US-AML identified and reported customers engaged in the Colombian ATM Typology. Nevertheless, the value of ATM withdrawals in Colombia using TDBNA accounts increased more than fivefold in three years, surging from \$28.6 million in 2018 to \$151.8 million

in 2021. In 2021 alone, a total of 12,227 TDBNA accounts had 675,570 ATM withdrawals in Colombia, a country in which TD Bank Group had no presence.

72. The Colombian ATM Typology continued at TDBNA until October 30, 2023, when—after law enforcement intervention—TDBNA began to identify and remove the five suspected insiders from its payroll and to institute systemic changes to prevent customers from engaging in the Colombian ATM Typology, including enhanced account opening controls, enhanced controls relating to debit card issuance, and reducing ATM withdrawal limits in certain countries, including Colombia.

73. Finally, even when TDBNA identified suspicious activity and decided to terminate customer relationships, the Bank often failed to carry out those terminations in a timely manner, thereby allowing billions of additional potentially suspicious funds to flow through the Bank. Throughout the relevant period, TDBNA maintained policies, procedures, and controls regarding the closure of accounts and termination of customer relationships based on AML risk, what TDBNA referred to as “demarketing.” Due to historical understaffing—resulting in part from the Bank’s “flat cost paradigm”—and repeated changes in demarketing procedures, TDBNA experienced frequent backlogs in its demarketing queue during the relevant period. In fact, for a significant portion of the relevant period, there was only one US-AML employee tasked with reviewing and dispositioning the thousands of annual Retail Requests to Close (“RTCs”), despite requests to Individual-2 to increase staffing on this project. These backlogs extended the period of time between the RTC submission and the actual account closure. From 2018 through 2021, on average, the demarketing process took nearly four months, with more complex cases averaging over five months from initial determination to account closure.

74. The practical effect of these persistent delays in demarketing was that, between 2018 and 2021, customers identified as outside of TDBNA's BSA/AML risk tolerance were regularly allowed to continue operating their accounts for months before they were finally closed. During the protracted timeframe between the initial determination and account closure, these customers conducted an additional \$5.16 billion in transaction activity through their TDBNA accounts. In fact, accounts involved in David's Network and MLO-2 conducted a total of \$168,375,555 in transaction activity *after* the Bank determined the accounts should be closed.

ATTACHMENT B

CERTIFICATE OF CORPORATE RESOLUTIONS

WHEREAS, TD BANK, N.A. (“TDBNA”) and TD BANK US HOLDING COMPANY (“TDBUSH”) (together, the “Defendants”), together with its legal counsel, have been engaged in discussions with the United States Department of Justice, Criminal Division, the Money Laundering and Asset Recovery Section (“MLARS”), and the United States Attorney’s Office for the District of New Jersey (the “USAO-DNJ”) (collectively, the “Offices”) in relation to the Offices’ investigation of violations of Title 18, United States Code, Section 371; Title 31, United States Code, Sections 5313, 5318(h), 5322, and 5324; and Title 18, United States Code, Section 1956 by the Defendants and certain of the Defendants’ employees and agents;

WHEREAS, in order to resolve such discussions, it is proposed that the Defendants enter into the Plea Agreements with the Offices (the “Agreements”);

WHEREAS, the Boards of Directors of the Defendants (the “Boards”) have had the opportunity to receive legal advice from the Defendants’ General Counsel, Cynthia Adams, together with outside counsel for the Defendants, in respect of the terms of the Agreements and of the Defendants’ rights, the possible defenses, the Sentencing Guidelines’ provisions, and the consequences of entering into such Agreements with the Offices;

NOW, THEREFORE BE IT RESOLVED by the Boards that:

1. The Defendants (a) acknowledge the filing of the one-count Information charging TDBNA with conspiring to: (i) fail to establish, implement, and maintain an appropriate anti-money laundering (“AML”) program, contrary to Title 31, United States Code, Sections 5318(h) and 5322, (ii) fail to file accurate Currency Transaction Reports (“CTRs”), contrary to Title 31, United States Code, Sections 5313 and 5324, and (iii) launder monetary instruments, contrary to

Title 18 United States Code, Section 1956(a)(2)(B)(i), in violation of Title 18 United States Code, Section 371, and the two-count Information charging TDBUSH with failing to (1) establish, implement, and maintain an appropriate AML program, in violation of Title 31, United States Code, Sections 5318(h) and 5322 and (2) file accurate CTRs in violation of Title 31, United States Code, Sections 5313 and 5324; (b) waive indictment on such charges and enter into the Agreements with the Offices; (c) agree to pay a fine of \$1,434,513,478.40; (d) agree to accept a Total Criminal Forfeiture/Money Judgment of \$452,432,302; (e) admit the Court's jurisdiction over the Defendants and the subject matter of such action and consent to the judgments therein; and (f) agree to undertake certain compliance, monitor, and disclosure obligations as set forth in the Agreements;

2. The Defendants accept the terms and conditions of the Agreements, including, but not limited to: (a) a knowing waiver of their rights to a speedy trial pursuant to the Sixth Amendment to the United States Constitution, Section 3161 of Title 18 of the United States Code, and Federal Rule of Criminal Procedure 48(b); (b) a knowing waiver for purposes of the Agreements and any charges by the United States arising out of the conduct described in the Statement of Facts attached to the Agreements of any objection with respect to venue and consent to the filing of the Informations, as provided under the terms of the Agreements, in the United States District Court for the District of New Jersey; 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 Agreements and Informations or relating to conduct known to the Offices prior to the date on which these Agreements are signed that is not time-barred by the applicable statute of limitations on the date of the signing of these Agreements;

3. The General Counsel of TDBNA and TDBUSH, Cynthia Adams, is hereby

authorized, empowered, and directed, on behalf of the Defendants, to execute the Agreements substantially in such form as reviewed by the Boards, with such changes as General Counsel of TDBNA and TDBUSH, Cynthia Adams, may approve;

4. The General Counsel of TDBNA and TDBUSH, Cynthia Adams, 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 agreements 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 General Counsel of TDBNA and TDBUSH, Cynthia Adams, which 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 Defendants.

Date: _____

By: _____



Mark Chauvin, Chairman of the Board
TD BANK, N.A.

CERTIFICATE OF CORPORATE RESOLUTIONS

WHEREAS, TD BANK, N.A. (“TDBNA”) and TD BANK US HOLDING COMPANY (“TDBUSH”) (together, the “Defendants”), together with its legal counsel, have been engaged in discussions with the United States Department of Justice, Criminal Division, the Money Laundering and Asset Recovery Section (“MLARS”), and the United States Attorney’s Office for the District of New Jersey (the “USAO-DNJ”) (collectively, the “Offices”) in relation to the Offices’ investigation of violations of Title 18, United States Code, Section 371; Title 31, United States Code, Sections 5313, 5318(h), 5322, and 5324; and Title 18, United States Code, Section 1956 by the Defendants and certain of the Defendants’ employees and agents;

WHEREAS, in order to resolve such discussions, it is proposed that the Defendants enter into the Plea Agreements with the Offices (the “Agreements”);

WHEREAS, the Boards of Directors of the Defendants (the “Boards”) have had the opportunity to receive legal advice from the Defendants’ General Counsel, Cynthia Adams, together with outside counsel for the Defendants, in respect of the terms of the Agreements and of the Defendants’ rights, the possible defenses, the Sentencing Guidelines’ provisions, and the consequences of entering into such Agreements with the Offices;

NOW, THEREFORE BE IT RESOLVED by the Boards that:

6. The Defendants (a) acknowledge the filing of the one-count Information charging TDBNA with conspiring to: (i) fail to establish, implement, and maintain an appropriate anti-money laundering (“AML”) program, contrary to Title 31, United States Code, Sections 5318(h) and 5322, (ii) fail to file accurate Currency Transaction Reports (“CTRs”), contrary to Title 31, United States Code, Sections 5313 and 5324, and (iii) launder monetary instruments, contrary to Title 18 United States Code, Section 1956(a)(2)(B)(i), in violation of Title 18 United States Code,

Section 371, and the two-count Information charging TDBUSH with failing to (1) establish, implement, and maintain an appropriate AML program, in violation of Title 31, United States Code, Sections 5318(h) and 5322 and (2) file accurate CTRs in violation of Title 31, United States Code, Sections 5313 and 5324; (b) waive indictment on such charges and enter into the Agreements with the Offices; (c) agree to pay a fine of \$1,434,513,478.40; (d) agree to accept a Total Criminal Forfeiture/Money Judgment of \$452,432,302; (e) admit the Court's jurisdiction over the Defendants and the subject matter of such action and consent to the judgments therein; and (f) agree to undertake certain compliance, monitor, and disclosure obligations as set forth in the Agreements;

7. The Defendants accept the terms and conditions of the Agreements, including, but not limited to: (a) a knowing waiver of their rights to a speedy trial pursuant to the Sixth Amendment to the United States Constitution, Section 3161 of Title 18 of the United States Code, and Federal Rule of Criminal Procedure 48(b); (b) a knowing waiver for purposes of the Agreements and any charges by the United States arising out of the conduct described in the Statement of Facts attached to the Agreements of any objection with respect to venue and consent to the filing of the Informations, as provided under the terms of the Agreements, in the United States District Court for the District of New Jersey; 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 Agreements and Informations or relating to conduct known to the Offices prior to the date on which these Agreements are signed that is not time-barred by the applicable statute of limitations on the date of the signing of these Agreements;


8. The General Counsel of TDBNA and TDBUSH, Cynthia Adams, is hereby authorized, empowered, and directed, on behalf of the Defendants, to execute the Agreements

substantially in such form as reviewed by the Boards, with such changes as General Counsel of TDBNA and TDBUSH, Cynthia Adams, may approve;

9. The General Counsel of TDBNA and TDBUSH, Cynthia Adams, 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 agreements or other documents as may be necessary or appropriate to carry out and effectuate the purpose and intent of the foregoing resolutions; and

10. All of the actions of the General Counsel of TDBNA and TDBUSH, Cynthia Adams, which 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 Defendants.

Date: _____

By:  _____
Mark Chauvin, Chairman of the Board
TD BANK US HOLDING COMPANY

ATTACHMENT C

COMPLIANCE COMMITMENTS

In order to address any deficiencies in its compliance programs, policies, procedures, codes of conduct, systems, and internal controls regarding compliance with the Bank Secrecy Act, 31 U.S.C. §§ 5311, et seq. (the “BSA”), anti-money laundering (“AML”) laws and regulations, and money laundering laws, TD BANK, N.A. (“TDBNA”) and TD BANK US HOLDING COMPANY (“TDBUSH”) (together, the “Defendants”), on behalf of themselves and their subsidiaries and affiliates involved in banking activity in the United States, agree to conduct in a manner consistent with all of their obligations under this Agreement appropriate reviews of their existing compliance programs, policies, procedures, codes of conduct, systems, and internal controls as they relate to the BSA, AML laws and regulations, and money laundering laws (the “Compliance Programs”). The Toronto-Dominion Bank (doing business as “TD Bank Group”) and TD Group US Holdings LLC (“TDGUS” and, with TD Bank Group, the “Parents”) agree to ensure that the Defendants comply with the commitments set forth in this Attachment.

Where necessary and appropriate, the Defendants agree to adopt new or to enhance existing programs, policies, procedures, codes of conduct, systems, and internal controls to ensure the Defendants comply with the BSA and AML laws and implements and maintain Compliance Programs that guard against money laundering and the financing of terrorism, including by detecting, deterring, and preventing illicit transactions at the Defendants. At a minimum, this will include, but not be limited to, the following elements to the extent they are not already part of the Defendants’ existing Compliance Programs:

High-Level Commitment to Compliance

1. The Defendants will ensure that members of the Parents' and the Defendants' Board of Directors, and the Parents' and the Defendants' directors and senior management provide strong, explicit, and visible support for and commitment to compliance with the Compliance Programs and demonstrate rigorous support for compliance via their words and actions. The Defendants and the Parents will also ensure that all levels of management reinforce that commitment to the Compliance Programs and encourage and incentivize employees to abide by the Compliance Programs. The Defendants and the Parents will create and foster a culture of ethics and compliance with the law in its day-to-day operations at all levels of the Defendants.

Policies, Procedures, and Internal Controls

2. As part of its Compliance Programs, the Defendants will develop, promulgate, implement, and maintain clearly articulated and visible corporate policies, procedures, codes of conduct, systems, and internal controls designed to reduce the prospect of violations of the BSA and AML laws, and violations of money laundering laws. This corporate policy shall be memorialized in a written compliance code or codes. The Defendants will take appropriate measures to encourage and support the observance of ethics and the adherence to the Compliance Programs and related policies by personnel at all levels of the Defendants. The Compliance Programs shall apply to all directors, officers, and employees of the Defendants and, where necessary and appropriate, outside parties acting on behalf of the Defendants, including but not limited to agents and intermediaries, consultants, representatives, distributors, licensees, contractors and suppliers, and joint venture partners (collectively, "agents and business partners"). The Defendants and their Parents shall notify all employees that compliance with the Compliance Programs is the duty of individuals at all levels of the Defendants.

3. The Compliance Programs shall address, among others, the following minimum requirements:

- a. designation of high-risk customers;
- b. appropriate procedures for know-your-customer and customer due diligence to verify customer and beneficial owner information when opening accounts;
- c. reviews of high-risk customer accounts;
- d. periodic account and accountholder reviews for illicit activity and money laundering risk;
- e. automated transaction monitoring for suspicious or unlawful activity;
- f. periodic threshold testing and analysis of transaction monitoring scenarios, including but not limited to review of transaction monitoring scenarios to address new product lines or risk areas, scenarios identified by regulators or the Defendants as suspicious, and the scope and coverage of transaction monitoring and any transaction monitoring gaps;
- g. creation and implementation of transaction monitoring scenarios to address risks, including risks presented by new products and services;
- h. review of suspicious activity;
- i. review of internal reports of unusual transactions or activities, including but not limited to unusual transaction referrals (“UTRs”);
- j. timely and appropriate closure, or demarketing, of customer accounts;
- k. timely response to law enforcement requests and legal process;
- l. timely and complete filing of suspicious activity reports (“SARs”);
- m. timely and complete filing of currency transaction reports (“CTRs”);
- n. periodic threshold testing and analysis of CTR thresholds;

o. policies and procedures to mitigate insider risk as it relates to the BSA, laws prohibiting money laundering, other laws against illicit finance, and laws prohibiting bribery of bank employees and theft of customer information and funds, including risks presented by gifts and bribes;

p. periodic and independent audit of the Compliance Programs, to be conducted by the Defendants' internal audit function or an outside party;

q. designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance, and provision to that individual of appropriate authority and reporting to senior management;

r. designation of an individual and/or department with ownership of each procedure, system, and internal control;

s. internal reporting process of compliance issues;

t. independence of compliance function from the business line;

u. routine assessment of resources required to implement and maintain effective Compliance Programs and to review whether the necessary resources have, in fact, been committed to the Compliance Programs;

v. process for reporting appropriate Compliance Programs information to the Defendants' or Parents' Board of Directors;

w. process for reporting information to regulators;

x. whistleblower procedures and protections; and

y. employee training, including review of existing employee training and understanding related to the Compliance Program and implementation of new, enhanced, or additional training and guidance where appropriate;

Transaction Monitoring and Reporting

4. As part of the Compliance Programs, the Defendants will institute and enhance its transaction monitoring program, to ensure a transaction monitoring program that includes automated features and is adaptive to identified risks, including risks identified internally at the Defendants, by regulators, from review of publicly available information, and from law enforcement referrals or inquiries. The Defendants will ensure the transaction monitoring program is informed by its risk profile and appropriately accounts for the areas of greatest risk, with particular emphasis on higher-risk products, services, customers, and geographies. The Defendants will regularly review the transaction monitoring program, including its scope, resources, and coverage, and update, test, and tune the transaction monitoring program as needed to ensure it appropriately addresses risk areas.

5. The Defendants will institute and enhance policies, procedures, and processes for managing alerts identified by its transaction monitoring program, including but not limited to evaluating UTRs, making decisions on SARs, completing and filing SARs, and monitoring and filing SARs on continuing activity. The Defendants will ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities and that part of this review and reporting includes review of customer due diligence and know your customer materials to assess whether activity is suspicious.

6. The Defendants will establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects when appropriate, identifying unusual or potentially suspicious activity related to those subjects, and filing, as appropriate, SARs related to those subjects.

7. The Defendants will establish policies, procedures, and systems to ensure that assigned personnel file accurate and comprehensive CTRs on all transactions that meet the established parameters.

8. The Defendants will generate reports for management review of patterns or outliers in transaction activity, and shall consider, for example, CTR summary reports, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports, change in behavior reports, and ATM transaction reports. Defendants' management will select filtering criteria and thresholds to produce such transaction reports, subject to periodic review and approval, that will enable the Defendants to detect potential patterns and typologies of unusual activity and management to receive reports of that activity.

9. The Defendants' transaction monitoring systems will be independently tested and reviewed for reasonable filtering criteria and thresholds, which review could be included in periodic independent audit of the Compliance Programs and functions.

Customer and Third-Party Relationships

10. As part of the Compliance Programs, the Defendants will institute and enhance appropriate, risk-based customer identification, due diligence, and compliance procedures that are written and approved by the Defendants pertaining to the acceptance, retention, and oversight of all accountholders, including, among others, the following minimum requirements:

a. procedures for verifying the identity of each customer to form a reasonable belief that it knows the true identity of the customer, including account-opening procedures detailing the identifying information to obtain from each customer and procedures detailing the use of non-documentary methods to verify the identity of the customer, including, for example: contacting a customer; comparing information provided by the customer with information obtained

from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement;

b. procedures for making and maintaining a record of all information obtained to identify and verify a customer's identity;

c. as part of its Compliance Programs, policies, procedures, and internal controls related to the Defendants' customer identification and due diligence designed to mitigate and manage money laundering, terrorism financing, and other illicit financial activity risks;

d. procedures for periodic review of customer accounts;

e. properly documented procedures for closing customer accounts; and

f. procedures for retaining and sharing information regarding customers and transactions within the Defendants and with third parties, including law enforcement, to the extent permissible under applicable law.

Proper Oversight and Independence

11. The Defendants will assign responsibility to one or more members of senior management at the Defendants for the implementation and oversight of the Defendants' Compliance Programs. Such members of senior management shall be highly qualified and experienced within the field; shall have the authority to report directly to independent monitoring bodies, including internal audit, and any appropriate management committee or executive of the Defendants or the Parents; and shall have an adequate level of autonomy from management as well as sufficient resources and authority to maintain such autonomy. The duties and responsibilities of such individuals with assigned responsibility for the implementation and oversight of the

Defendants' Compliance Programs shall be documented, approved, and subject to periodic review by the Defendants and the Parents.

Insider Risk

12. The Defendants will implement and maintain insider risk controls designed to prevent and deter circumvention of the Compliance Programs and violations of law through the Defendants by employees at all levels of the Defendants. These controls will achieve, among others, the following minimum requirements:

- a. prevent and deter employees from accessing or using the Defendants' systems in an unauthorized or illicit manner;
- b. prevent and deter employees from accessing or using customer accounts in an unauthorized or illicit manner;
- c. prevent and deter employees from soliciting or receiving bribes, kickbacks, gratuities, or gifts in exchange for conducting certain activities from inside the Defendants; and
- d. prevent and deter employees from conducting or processing transactions in a manner designed to circumvent the Compliance Programs, including the Defendants' reporting requirements pursuant to the BSA.

Training and Guidance

13. The Defendants will implement and enhance mechanisms to effectively communicate its Compliance Programs and all related ethics and compliance policies to all directors, officers, employees, and, where necessary and appropriate, agents and business partners. These mechanisms shall include: (a) periodic training for all directors and officers, all employees in positions of leadership or trust, all employees in positions that require targeted training (e.g., internal audit, legal, compliance, retail), and, where necessary and appropriate, agents and business

partners; (b) certifications of compliance with training requirements by all directors, officers, employees, and agents and business partners that are subject to the periodic training; and (c) reporting on training requirements and programs to senior management of the Defendants and the Parents.

14. The Defendants will provide supplemental training to directors, officers, employees, and, where necessary and appropriate, agents and business partners, when such training is warranted to ensure compliance with the Defendants' Compliance Programs and all related ethics and compliance policies. Such circumstances for supplemental training may include, for example, emerging typologies, evolving industry standards, technological developments, and other developments in the field relevant to the adequacy of the Compliance Programs. In such circumstances, the Defendants will obtain certifications of compliance with the training requirements from such individuals subject to the supplemental training.

15. The Defendants will establish an effective policy, procedure, or system for providing guidance and advice to directors, officers, employees, and, where necessary and appropriate, agents and business partners, on complying with the Defendants' Compliance Programs and all related ethics and compliance policies, and addressing violations of law or the Compliance Programs, including a channel for guidance and advice on an urgent basis.

Internal Reporting and Investigation

16. The Defendants will implement and maintain a system for internal and, where possible, confidential reporting by, directors, officers, employees, and applicable agents and business partners of alleged violations of the Compliance Programs, the BSA, and laws prohibiting money laundering and other forms of illicit finance. Such system shall include protections against

retaliation for the reporting directors, officers, employees, and applicable agents and business partners.

17. The Defendants will implement and maintain mechanisms designed to ensure that the system for internal reporting of alleged violations and the related protections against retaliation are effectively communicated to all directors, officers, employees, and applicable agents and business partners.

18. The Defendants will implement and maintain an effective and reliable process with sufficient resources for responding to, investigating, documenting, and resolving allegations of violations of the Compliance Programs, the BSA, and laws prohibiting money laundering and other forms of illicit finance.

Enforcement and Discipline

19. The Defendants will implement and enhance mechanisms designed to effectively enforce the Compliance Programs and all related ethics and compliance policies. Such mechanisms shall appropriately incentivize compliance and discipline violations.

20. The Defendants will institute appropriate disciplinary procedures to address, among other things, violations of the Compliance Programs, the BSA, and laws prohibiting money laundering and other forms of illicit finance by the Defendants' directors, officers, and employees. To the extent the Defendants determine that such violations implicate directors, officers, and employees of the Parents, the Parents will also adopt appropriate disciplinary procedures. Such procedures should be applied consistently and fairly, regardless of the position held by or perceived authority of the director, officer, or employee.

21. The Defendants shall implement procedures to ensure that, where an above-stated violation is discovered, reasonable steps are taken to remedy the harm resulting from such violation

and to prevent future similar violations, including, for example, by assessing the Compliance Programs and implementing modifications to the Compliance Programs as necessary to ensure the Compliance Programs are effective.

Compliance Incentives

22. The Defendants will ensure that their compensation and bonus systems are designed to incentivize adherence to the Defendants' Compliance Programs and any related ethics and compliance policies designed to prevent violations of the BSA and laws prohibiting money laundering and other forms of illicit finance. To the extent that directors, officers, or employees of the Parents are engaged in duties governed by the Compliance Programs, the Parents will also implement such incentives. These include the following minimum requirements:

- a. prohibitions on bonuses for directors, officers, and employees who do not satisfy compliance performance requirements;
- b. compensation reduction provisions permitting the Defendants and the Parents to seek to recoup compensation paid to directors, officers, and employees who (i) commit an above-stated violation, or (ii) have supervisory authority over employee(s) or business area(s) related to or involved in the commission of an above-stated violation and knowledge of, or willfully blindness to, the violation; and
- c. criteria related to compensation and bonus incentives for employees who demonstrate full commitment to compliance processes.

23. The Defendants will not permit any person to participate, directly or indirectly, formally or informally, in managing, performing, or conducting the operations of the Defendants who has been convicted of a crime related to the conduct set forth in the Statement of Facts.

Monitoring, Testing, and Audit

24. The Defendants will conduct periodic reviews and testing of the Compliance Programs designed to evaluate and improve their effectiveness in complying with the BSA and in preventing and detecting violations of laws prohibiting money laundering and other forms of illicit finance.

25. Such reviews and testing by the Defendants will involve risk-based assessments of the individual circumstances of the Defendants, and particularly the money laundering risks facing the Defendants, including, but not limited to, its high-cash customer accounts, foreign ATM withdrawal activity, peer-to-peer payment platform activity, evolving industry standards, and any other emerging typologies.

26. In concert with such reviews and testing, the Defendants shall review and update its Compliance Programs as appropriate, and no less than annually, to ensure their continued effectiveness and risk-tailored resource allocation, considering lessons learned, relevant developments in the industry, and evolving industry standards. The updated Compliance Programs shall be subject to review and approval by the appropriate board of directors and/or board committee(s) of the Defendants and the Parents.

27. The Defendants will ensure that the testing and audit functions are accountable to senior management of the Defendants and the Parents, are independent of the tested or audited activities and functions, and have sufficient authority, skills, expertise, resources, and authority within the organization to effectively review and test the Compliance Programs for compliance with the BSA and laws prohibiting money laundering and other forms of illicit finance.

28. The Defendants will ensure that it employs testing or audit procedures appropriate to the level and sophistication of the Compliance Programs and that this function, whether

deployed internally or by an external party, reflects a comprehensive and objective assessment of the Defendants' Compliance Programs for compliance with the BSA and laws prohibiting money laundering and other forms of illicit finance.

29. The Defendants will implement and maintain procedures designed to ensure that, upon learning of an adverse testing result or audit finding pertaining to its Compliance Programs, the Defendants take timely and effective action to identify and implement compensating controls until the root cause of the adverse testing result or audit finding can be determined and remediated.

ATTACHMENT D

INDEPENDENT COMPLIANCE MONITOR

As set forth in the Plea Agreement (the “Agreement”), TD BANK, N.A. (“TDBNA”) and TD BANK US HOLDING COMPANY (“TDBUSH”) (together, the “Defendants”) have agreed to retain an independent compliance monitor (the “Monitor”). The duties and authority of the Monitor and the obligation of the Defendants with respect to the Monitor and the United States Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section (“MLARS”) and the United States Attorney’s Office for the District of New Jersey (“USAO-DNJ”) (together, the “Offices”) are as described below.

1. The Defendants will retain the Monitor, in accordance with the procedure established in the Agreement, for a period of three years (the “Term of the Monitorship” or the “Term”) unless the provision for extension described in Paragraph 7 of the Agreement is triggered.

Monitor’s Mandate

2. The Monitor’s primary responsibility is to assess and monitor the Defendants’ compliance with the terms of the Agreement, including the adequacy of the Defendants’ Bank Secrecy Act/anti-money laundering (“BSA/AML”) compliance programs, other existing compliance programs, policies, procedures, codes of conduct, systems, and internal controls (the “Compliance Programs”), as described in Attachment C, to specifically remediate the deficiencies that resulted in the misconduct described in the Statement of Facts and to address and reduce the risk of any recurrence by the Defendants of such misconduct. During the Term of the Monitorship, the Monitor will evaluate, in the manner set forth below, the effectiveness of the Defendants’ Compliance Programs, particularly as they relate to the Defendants’ current and ongoing compliance with the BSA and related anti-money laundering laws and regulations and laws prohibiting money laundering and other forms of illicit finance. In so doing, the Monitor will take

such reasonable steps as, in their view, may be necessary to fulfill the foregoing mandate (the “Mandate”). This Mandate shall include an assessment of the Defendants’ parents, Toronto-Dominion Bank (“TD Bank Group”) and TD Group US Holdings LLC (“TDGUS”), and the Board of Directors’ and senior management’s commitments to, and effective oversight of the implementation of, the compliance commitments described in Attachment C of the Agreement.

Defendants’ Obligations

3. The Defendants shall cooperate fully with the Monitor, and the Monitor shall have the authority to take such reasonable steps as, in their view, may be necessary to be fully informed about the Defendants’ Compliance Programs in accordance with the principles set forth herein and subject to applicable law, including applicable bank secrecy, data protection and labor laws and regulations. To that end, except as provided in Paragraphs 5 and 6 below, the Defendants, including any subsidiaries, parents, affiliates, or joint ventures, shall provide the Monitor with full access to all information, documents, records, facilities, and employees, as reasonably requested by the Monitor, that fall within the scope of the Mandate of the Monitor, including information, documents, records, facilities, and employees outside the United States. Defendants shall use their best efforts to provide the Monitor with full access to the Defendants’ former employees, agents, intermediaries, consultants, representatives, distributors, licensees, contractors, suppliers, and joint venture partners (collectively, “agents and business partners”), as reasonably requested by the Monitor, that fall within the scope of the Mandate of the Monitor. The Defendants shall inform, as necessary, agents and business partners of this obligation.

4. Any disclosure by the Defendants to the Monitor concerning violations of the BSA and laws prohibiting money laundering and other forms of illicit finance shall not relieve the Defendants of any otherwise applicable obligation to truthfully disclose such matters to the Offices pursuant to the Agreement.

Withholding Access

5. The Defendants and the Monitor agree that no attorney-client relationship shall form between the Defendants and the Monitor. In the event that the Defendants seek to withhold from the Monitor access to information, documents, records, facilities, employees, or agents and business partners of the Defendants pursuant to a potential claim of attorney-client privilege or the attorney work-product doctrine, or where the Defendants reasonably believe production would otherwise be inconsistent with applicable law, the Defendants shall work cooperatively with the Monitor to resolve the matter to the satisfaction of the Monitor.

6. If the matter cannot be resolved, at the request of the Monitor, the Defendants shall promptly provide written notice to both the Monitor and the Offices containing a general description of the nature of the information, documents, records, facilities, employees, or agents and business partners that are being withheld and the legal basis for such withholding. The Offices may then consider whether to make a further request for access to such information, documents, records, facilities, employees, or agents and business partners pursuant to the cooperation provisions set forth in Paragraph 10 of the Agreement.

Monitor's Coordination with the Defendants and Review Methodology

7. In carrying out the Mandate, to the extent appropriate under the circumstances, the Monitor should coordinate with Defendants' personnel, including in-house counsel, compliance personnel, and internal auditors, on an ongoing basis. The Monitor may rely on the Defendants' internal resources (e.g., legal, compliance, and internal audit), which can assist the Monitor in carrying out the Mandate with efficiency and Defendants'-specific expertise, and the products of the Defendants' processes, including the results of reviews, sampling and testing, audits, and analyses conducted by or on behalf of the Defendants, provided that the Monitor has confidence in the quality and reliability of those resources and products.

8. The Monitor should take a risk-based approach to conducting reviews, and thus, is not expected to conduct a comprehensive review of all business lines, all business activities, or all markets. In carrying out the Mandate, the Monitor should consider, for instance, risks presented by the following, among other, factors:

- a. The countries and business areas in which the Defendants operate or in which their customers are located;
- b. The size of the Defendants and the volume of their business;
- c. The nature and volume of the financial services provided the Defendants;
- d. The nature of the Defendants' customers, including the customers' stated lines of business, intended purpose for each account, and estimated cash and transaction volumes;
- e. The quality and quantity of compliance resources at the Defendants;
- f. The adequacy of employee resources, including employee compliance training, internal mechanisms for reporting misconduct or suspicious activity, and mechanisms for review of insider risk and deterrence of employee misconduct;
- g. The technological limitations of the respective procedures and systems at the Defendants;
- h. The automated or manual nature of the respective procedures and systems at the Defendants;
- i. The centralized or decentralized nature of the respective procedures and systems at the Defendants; and
- j. The Defendants' misconduct as described in the Statement of Facts, including their failure to maintain adequate Compliance Programs, and conduct appropriate employee training and risk monitoring.

9. In undertaking its reviews, the Monitor shall formulate conclusions based on, among other things:

- a. Inspection of relevant documents, including the Defendants' current compliance policies and procedures;
- b. Direct observation of selected procedures and systems at the Defendants, including those related to transaction monitoring, suspicious activity reporting, currency transaction reporting, compliance training, internal control testing, and internal audit functions;
- c. Meetings with, and interviews of, relevant current and, where appropriate, former shareholders, officers, employees, agents and business partners, and other persons at mutually convenient times and places; and
- d. Analyses, studies, and testing of the Compliance Programs.

Monitor's Review Process and Written Work Plans

10. To carry out the Mandate, the Monitor shall conduct a series of reviews, starting with a written work plan prior to start of the review and ending with a written report based on the review.

11. The Monitor's first task will be to prepare a written work plan for the first review. After consultation with the Defendants and the Offices and within sixty (60) calendar days of being retained, the Monitor shall submit to the Defendants and the Offices the first written work plan. The Defendants and the Offices shall provide comments on the first written work plan within thirty (30) calendar days after receipt. Any dispute between the Defendants and the Monitor with respect to any written work plan shall be settled by the Offices in their sole discretion.

12. The Monitor will conduct at least two follow-up reviews, as described in Paragraphs 18 through 23 below. The Monitor shall prepare and submit each follow-up written work plan to the Defendants and the Offices after consultation with the Defendants and the Offices

and at least thirty (30) calendar days prior to commencing the follow-up review. The Defendants and the Offices shall provide comments on each follow-up written work plan within twenty (20) calendar days after receipt. Any dispute between the Defendants and the Monitor with respect to any written work plan shall be settled by the Offices in their sole discretion.

13. All written work plans shall identify with reasonable specificity the activities the Monitor plans to undertake in its review pursuant to the Mandate, including a written request to the Defendants for documents. The Monitor's first written work plan shall include such steps as are reasonably necessary to conduct an effective initial review in accordance with the Mandate, including developing an understanding, to the extent the Monitor deems appropriate, of the facts and circumstances surrounding any violations that may have occurred before the date of the Agreement. In developing such understanding, the Monitor is to rely, to the extent possible, on available information and documents provided by the Defendants. It is not intended that the Monitor will conduct their own inquiry or investigation into the historical events that gave rise to the Agreement.

First Review & Written Report

14. The first review shall commence no later than one hundred twenty (120) calendar days from the date of the engagement of the Monitor (unless otherwise agreed by the Defendants, the Monitor, and the Offices). The Monitor shall issue a first written report within one hundred fifty calendar (150) days of commencing the first review, setting forth the Monitor's assessment and, as applicable, making recommendations reasonably designed to improve the effectiveness of the Defendants' Compliance Programs as defined in Attachment C. The Monitor should consult with the Defendants concerning the Monitor's findings and recommendations on an ongoing basis and should consider the Defendants' comments and input to the extent the Monitor deems appropriate. The Monitor may also choose to share its draft written reports with the Defendants

before finalizing. The Monitor's written reports need not recite or describe comprehensively the Defendants' history or compliance policies, procedures, and practices. Rather, the reports should focus on areas the Monitor has identified as requiring improvement or which the Monitor otherwise concludes merit particular attention. The Monitor shall provide each report to the Defendants' governing authority and contemporaneously transmit copies to the following representatives of the Offices or their designees (including electronically, if requested by the Offices):

Chief and Deputy Chief, Bank Integrity Unit
Money Laundering and Asset Recovery Section, Criminal Division
U.S. Department of Justice
Bond Building, Tenth Floor
1400 New York Avenue, N.W.
Washington, DC 20005

U.S. Attorney and First Assistant U.S. Attorney
United States Attorney's Office for the District of New Jersey
970 Broad Street
Newark, NJ 07102

After consultation with the Defendants and with prior written approval of the Offices, the Monitor may extend the deadline for issuance of the first written report for a reasonable amount of time.

15. Within one hundred fifty (150) calendar days after receiving the Monitor's first report, the Defendants shall adopt and implement all recommendations in the report. If the Defendants consider any recommendations inconsistent with applicable law or regulation, impractical, excessively expensive, unduly burdensome, or otherwise inadvisable, they must notify the Monitor and the Offices of any such objections to recommendations in writing within sixty (60) calendar days of receiving the report. The Defendants shall include in such written notification a proposal to the Monitor and the Offices of an alternative policy, procedure, or system designed to achieve the same objective or purpose of the contested recommendation. The Defendants need

not adopt the contested recommendations within the allotted one hundred fifty (150) calendar days. As to any recommendation on which the Defendants and the Monitor do not agree, such parties shall attempt in good faith to reach an agreement within forty-five (45) calendar days after the Defendants serve the written notice. If agreement between the Defendants and the Monitor is reached, the Defendants shall adopt and implement the agreed-upon recommendation within ninety (90) calendar days after reaching such agreement.

16. In the event the Defendants and the Monitor are unable to agree on an acceptable alternative proposal within the forty-five (45) calendar days after the Defendants' notice, the Defendants and the Monitor shall promptly consult with the Offices. The Offices may consider the Monitor's recommendation and the Defendants' reasons for objecting to the recommendation in determining whether the Defendants has fully complied with their obligations under the Agreement. Pending a determination by the Offices, the Defendants shall not be required to implement any contested recommendations.

17. With respect to any recommendation that the Monitor determines cannot reasonably be implemented by the Defendants within one hundred fifty (150) calendar days after delivering the written report, the Monitor may extend the time for implementation with prior written approval of the Offices.

Second Review & Written Report

18. The Monitor shall commence the second review no later than one hundred eighty (180) calendar days after the issuance of the first written report (unless otherwise agreed by the Defendants, the Monitor, and the Offices). As outlined in Paragraph 12 above, the Monitor shall submit the second and subsequent written work plans at least thirty (30) calendar days prior to commencing the related follow-up review. The Monitor shall issue the second written report within one hundred twenty (120) calendar days of commencing review, setting forth the Monitor's

assessment and, as applicable, making recommendations following the procedures set forth in Paragraph 13 above. After consultation with the Defendants and with prior written approval of the Offices, the Monitor may extend the deadline for issuance of the second written report for a reasonable amount of time.

19. Within one hundred twenty (120) calendar days after receiving the Monitor's second report, the Defendants shall adopt and implement all recommendations in the report, unless, within thirty (30) calendar days after receiving the report, the Defendants notify the Monitor and the Offices in writing that the Defendants consider a recommendation inconsistent with applicable law or regulation, impractical, excessively expensive, unduly burdensome, or otherwise inadvisable. The Defendants shall include in such written notification a proposal to the Monitor and the Offices of an alternative policy, procedure, or system designed to achieve the same objective or purpose of the contested recommendation. The Defendants need not adopt a contested recommendation within the allotted one hundred twenty (120) calendar days. As to any recommendation on which the Defendants and the Monitor do not agree, such parties shall attempt in good faith to reach an agreement within thirty (30) calendar days after the Defendants serve the written notice. If agreement between the Defendants and the Monitor is reached, the Defendants shall adopt and implement the agreed-upon recommendation within ninety (90) calendar days after reaching such agreement.

20. In the event the Defendants and the Monitor are unable to agree on an acceptable alternative proposal within the thirty (30) calendar days after the Defendants' notice, the Defendants and the Monitor shall promptly consult with the Offices. The Offices may consider the Monitor's recommendation and the Defendants' reasons for objecting to the recommendation in determining whether the Defendants have fully complied with their obligations under the

Agreement. Pending a determination by the Offices, the Defendants shall not be required to implement any contested recommendations.

21. With respect to any recommendation that the Monitor determines cannot reasonably be implemented by the Defendants within one hundred twenty (120) calendar days after delivering the written report, the Monitor may extend the time for implementation with prior written approval of the Offices.

Third Review & Written Report

22. The Monitor shall commence the third review no later than one hundred fifty (150) calendar days after the issuance of the second written report (unless otherwise agreed by the Defendants, the Monitor, and the Offices), with the third written work plan due at least thirty (30) calendar days prior to commencing the third review. The Monitor shall issue the third written report within one hundred twenty (120) calendar days of commencing review, and recommendations and any objections shall follow the same timelines and procedures set forth in Paragraphs 18 through 21 above. After consultation with the Defendants and with prior written approval of the Offices, the Monitor may extend the deadline for issuance of the third written report for a reasonable amount of time.

23. Following the third review, the Monitor shall certify in a final review and report whether the Defendants' Compliance Programs, including their policies, procedures, codes of conduct, systems, and internal controls, are reasonably designed and implemented to prevent and detect violations of the BSA, laws prohibiting money laundering, and laws prohibiting other forms of illicit finance. A final review and report containing such certification shall be completed and delivered to the Offices no later than thirty (30) days before the end of the Term of the Monitorship. If, after the third review, the Monitor assesses that the Defendants' Compliance Programs are not reasonably designed and implemented to prevent and detect violations of the BSA, laws

prohibiting money laundering, and laws prohibiting other forms of illicit finance, the Offices may, in their sole discretion, declare a breach of the Agreement or an extension of the Term of the Monitorship in accordance with Paragraph 7 of the Agreement.

Monitor's Discovery of Potential or Actual Misconduct

24. Except as set forth below in sub-paragraphs (b), (c) and (d),

a. Should the Monitor discover "Potential Misconduct" during their Term, which means a high likelihood that, post-dating or not disclosed in the Agreement or Statement of Facts:

- i. An individual who has been convicted of a crime related to the conduct set forth in the Statement of Facts has participated, directly or indirectly, formally or informally, in the business of the Defendants, including managing, operating, or conducting Defendants' business;
- ii. The Defendants or their personnel have selectively enforced know-your-customer and customer due diligence policies and procedures;
- iii. The Defendants or their personnel have willfully failed to implement an effective anti-money laundering program;
- iv. Specific violations of the BSA, laws prohibiting money laundering, or laws prohibiting other forms of illicit finance may have occurred or may be ongoing;
- v. The Defendants or their personnel have knowingly permitted customer accounts to engage in unlawful activity, including conducting transactions with proceeds of unlawful activity;
- vi. Defendants' personnel have knowingly accepted a monetary payment or other non-*de minimis* compensation from a TDBNA customer or

third-party in return for a specified action or inaction;

- vii. The Defendants' technological controls to prevent circumvention of the Compliance Programs, described in Paragraph 7 of Attachment C, may be ineffective;
- viii. Real-time transaction and account monitoring may be ineffective;
- ix. The Defendants or their personnel may have maintained false books, records, or accounts; or
- x. The Defendants or their personnel have intentionally withheld relevant information from law enforcement or regulators,

the Monitor shall immediately report the Potential Misconduct to the Defendants' BSA Officer for further action unless the Potential Misconduct was already so disclosed. The Monitor will also immediately report Potential Misconduct to the Offices.

b. In some instances, the Monitor should immediately report Potential Misconduct to the Offices without reporting the Potential Misconduct to the Defendants. The presence of any of the following factors militates in favor of reporting Potential Misconduct to the Offices without reporting the Potential Misconduct to the Defendants, namely, where—in the Monitor's good faith assessment—the Potential Misconduct: (1) poses a risk to U.S. national security, public health or safety, or the environment; (2) involves senior management of the Defendants; (3) involves obstruction of justice or obstruction of a bank regulator; or (4) otherwise poses a substantial risk of harm.

25. The Monitor shall address in their reports the appropriateness of the Defendants' response to the Potential Misconduct. Further, if the Defendants or any entity or person working directly or indirectly for or on behalf of the Defendants withholds information necessary for the

performance of the Monitor's responsibilities and the Monitor believes that such withholding is without just cause, the Monitor shall immediately disclose that fact to the Offices and address the Defendants' failure to disclose the necessary information in their next written report.

26. Neither the Defendants, nor anyone acting on their behalf, shall take any action to retaliate against the Monitor for any such disclosures or for any other reason.

Meetings During Pendency of Monitorship

27. The Monitor shall meet with the Offices within thirty (30) calendar days after providing each written report to the Offices to discuss the report, to be followed by a meeting among the Offices, the Monitor, and the Defendants.

28. At least annually, and more frequently if the Offices deem it appropriate, representatives from the Defendants and the Offices will meet to discuss the Monitor and any suggestions, comments, or improvements the Defendants may wish to discuss with or propose to the Offices, including with respect to the scope or costs of the Monitor.

Contemplated Confidentiality of Monitor's Reports

29. The reports will likely include proprietary, financial, confidential, and competitive business information. Moreover, public disclosure of the reports could discourage cooperation, impede pending or potential government investigations, and undermine the objectives of the Monitorship. For these reasons, among others, the Monitor's written reports and the contents thereof are intended to remain and shall remain non-public, except as otherwise agreed to by the Defendants and the Monitor 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 respective duties and responsibilities or otherwise required by law.

ATTACHMENT E

DISCLOSURE 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
District of New Jersey
Attention: U.S. Attorney

Re: Plea Agreement Disclosure Certification

The undersigned certify, pursuant to Paragraph 11 of the Plea Agreements ("Agreements") filed on October 10, 2024 in the United States District Court for the District of New Jersey, by and between the United States Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section ("MLARS") and the United States Attorney's Office for the District of New Jersey ("the USAO-DNJ") (collectively the "Offices") and TD BANK, N.A. ("TDBNA") and TD BANK US HOLDING COMPANY ("TDBUSH") (collectively, the "Defendants"), that undersigned are aware of the Defendants' disclosure obligations under Paragraph 11 of the Agreements and that, to the best of the undersigned's knowledge and belief (including belief based on representations from others), the Defendants have complied with their disclosure obligations, as described in Paragraph 11 of the Agreements, which includes disclosure of evidence or allegations of conduct by the Defendants, their affiliates, or their employees that may constitute a violation of federal criminal law ("Disclosable Information"). This obligation to disclose information extends to any and all Disclosable Information that has been identified through the Defendants' anti-money laundering compliance program, sanctions compliance program, whistleblower channel, internal audit reports, due diligence procedures, investigative processes, or other systems and processes. The undersigned further acknowledge and agree that the reporting

requirement contained in Paragraph 11 and the representations contained in this Certification constitute a significant and important component of the Agreements and the Offices' determination of whether the Defendants have satisfied their obligations under the Agreements.

The undersigned hereby certify that they are respectively the Chief Executive Officer and BSA Officer of the Defendants and the Chief Executive Officer and Chief Anti-Money Laundering ("AML") Officer of TDBNA, TDBUSH, and the Toronto-Dominion Bank, d/b/a "TD Bank Group," and that each has been duly authorized by the Defendants to sign this Certification on behalf of the Defendants.

This Certification shall constitute a material statement and representation by the undersigned and by, on behalf of, and for the benefit of, the TDBNA, TDBUSH, and TD Bank Group 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 District of New Jersey. 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 District of New Jersey.

By: _____ Dated: _____
[Chief Executive Officer]
TD BANK, N.A.
TD BANK US HOLDING COMPANY

By: _____ Dated: _____
[BSA Officer]
TD BANK, N.A.
TD BANK US HOLDING COMPANY

By: _____
[Chief Executive Officer]
Toronto-Dominion Bank
d/b/a/ "TD Bank Group"

Dated: _____

By: _____
[Chief AML Officer]
Toronto-Dominion Bank
d/b/a/ "TD Bank Group"

Dated: _____

ATTACHMENT F

COMPLIANCE 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
District of New Jersey
Attention: U.S. Attorney

Re: Plea Agreement Compliance Certification

The undersigned certify, pursuant to Paragraphs 24 and 25 of TDBNA's Plea Agreement and Paragraphs 28 and 29 of TDBUSH's Plea Agreement (together, the "Agreements") filed on October 10, 2024 in the United States District Court for the District of New Jersey, by and between the United States Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section ("MLARS") and the United States Attorney's Office for the District of New Jersey ("the USAO-DNJ") (collectively the "Offices") and TD BANK, N.A. ("TDBNA") and TD BANK US HOLDING COMPANY ("TDBUSH") (together, the "Defendants"), that the undersigned are aware of the Defendants' compliance obligations pursuant to Paragraphs 24 and 25 of TDBNA's Plea Agreement, Paragraphs 28 and 29 of TDBUSH's Plea Agreement, and Attachment C to the Agreements and that, based on the undersigned's review and understanding of the Defendants' Compliance Program as defined in Attachment C, the Defendants have implemented a Compliance Program that meets the requirements set forth in Attachment C to the Agreements. The undersigned certify that the Defendants' Compliance Program is reasonably and effectively designed to detect and prevent violations of the Bank Secrecy Act and related regulations, money laundering laws, and laws prohibiting other forms of illicit finance throughout the Defendants' operations.

The undersigned hereby certify, if applicable, that, based on a review of the Defendants' reports submitted to the Offices, 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 and Bank Secrecy Act ("BSA") Officer of TDBNA and TDBUSH, the Chief Executive Officer and Chief Anti-Money Laundering ("AML") Officer of Toronto-Dominion Bank, d/b/a "TD Bank Group," and the Chief Executive Officer and Chief Risk Officer of TD Group US Holdings LLC ("TDGUS") and each has been duly authorized by the Defendants to sign this Certification on behalf of the Defendants.

This Certification shall constitute a material statement and representation by the undersigned and by, on behalf of, and for the benefit of, the TDBNA, TDBUSH, TDGUS, and TD Bank Group to the executive branch of the United States for purposes of Title 18, United States Code, Section 1001, and such material statement and representation shall be deemed to have been made in the District of New Jersey. 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 Title 18, United States Code, Section 1519, and such record, document, or tangible object shall be deemed to have been made in the District of New Jersey.

By: _____
[Chief Executive Officer]
TD BANK, N.A.
TD BANK US HOLDING COMPANY

Dated: _____

By: _____
[BSA Officer]
TD BANK, N.A.
TD BANK US HOLDING COMPANY

Dated: _____

By: _____
[Chief Executive Officer]
Toronto-Dominion Bank
d/b/a/ "TD Bank Group"

Dated: _____

By: _____
[Chief AML Officer]
Toronto-Dominion Bank
d/b/a/ "TD Bank Group"

Dated: _____

By: _____
[Chief Executive Officer]
TD Group US Holdings LLC

Dated: _____

By: _____
[Chief Risk Officer]
TD Group US Holdings LLC

Dated: _____

ATTACHMENT G

**CERTIFICATION OF TORONTO-DOMINION BANK AND TD GROUP US
HOLDINGS LLC**

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

United States Attorney's Office
District of New Jersey
Attention: U.S. Attorney

Re: Certification of Toronto-Dominion Bank and TD Group US Holdings LLC

Toronto-Dominion Bank, d/b/a "TD Bank Group" (the "Global Parent" or "TD Bank Group") and TD Group US Holdings LLC (the "U.S. Parent" or "TDGUS," and with TD Bank Group, the "Parents") hereby acknowledge that TD BANK, N.A. ("TDBNA") and TD BANK US HOLDING COMPANY ("TDBUSH") (together, the "Subsidiaries")—both wholly owned subsidiaries of the Parents—have agreed with the United States Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section ("MLARS") and the United States Attorney's Office for the District of New Jersey ("the USAO-DNJ") (collectively the "Offices") to plead guilty in the District of New Jersey pursuant to the attached Plea Agreements and to make other commitments as reflected in the Plea Agreements and their Attachments.

The Parents, which are not defendants in this matter, hereby agree:

(1) to undertake the cooperation commitments in the Plea Agreements and Attachments on behalf of the operations of TD Bank Group;

(2) to ensure the Subsidiaries fully comply with the terms and conditions agreed to in the Plea Agreements and Attachments—including but not limited to the cooperation, disclosure, compliance, and monitor commitments made in Paragraphs 7, 10-11, 24-25 of TDBNA's Plea

Agreement; Paragraphs 7, 10-11, and 28-29 of TDBUSH's Plea Agreement; and Attachments C and D to the Plea Agreements;

(3) to execute, through designated executives, Attachments E and F to the Plea Agreements at the end of the term of probation, certifying the Subsidiaries' compliance with the disclosure and compliance obligations in the Plea Agreements and Attachments;

(4) they shall not make or cause to be made, through their attorneys, boards of directors, agents, officers, employees, consultants, or authorized agents (including contractors, subcontractors, or representatives), including any person or entity controlled by any of them, any public statement contradicting or excusing any statement of fact contained in the Statement of Facts, and if it or any of their direct or indirect subsidiaries or affiliates make any affirmative public statement in connection with the Plea Agreements, including via press release, press conference remarks, or a scripted statement to investors, the Parents 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 Subsidiaries; and (b) whether the Offices have any objection to the release or statement;

(5) to agree to the undertakings regarding change in corporate form in Paragraph 9 of the Plea Agreements, including but not limited to ensuring that in the event of any change in corporate form, the successor in interest or purchaser agrees to the Plea Agreements and Statement of Facts, and the Parents notify the Offices of any anticipated change in corporate form;

(6) that in the event of a breach of the Plea Agreements, any prosecution relating to the conduct described in the Information and the Statement of Facts or relating to conduct known to the Offices prior to the date on which the Plea Agreements were signed that is not time-barred

by the applicable statute of limitations on the date of the signing of the Plea Agreements may be commenced against the Parents, notwithstanding the expiration of the statute of limitations, between the signing of this Plea Agreement and the expiration of the Term plus one year. Thus, the Parents agree that the statute of limitations with respect to any such prosecution that is not time-barred on the date of the signing of the Plea Agreement shall be tolled for the Term plus one year;

(7) that in the event of a breach of the Plea Agreements, any appropriate TD Bank entity shall thereafter be subject to prosecution for any federal criminal violation of which the Offices have knowledge, including, but not limited to, the charge(s) in the Informations described in Paragraphs 2 and 3 of the Plea Agreements, which may be pursued by the Offices in the U.S. District Court for the District of New Jersey or any other appropriate venue; and

(8) to voluntarily waive and give up the rights enumerated in Federal Rule of Criminal Procedure 11(f) and Federal Rule of Evidence 410 and agree that, as of the date TDBNA and TDBUSH sign the Plea Agreements, the Parents will not dispute the Statement of Facts and the Statement of Facts shall be admissible against the Parents in any criminal case involving the Offices 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. The Parents agree 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 Parents understand and agree that any statements that the Subsidiaries make in the course of their guilty pleas or in connection with the Plea Agreements are admissible against the Parents for any purpose in any U.S. federal criminal proceeding.

Failure to fully execute and comply with the above agreements shall be the basis for a breach of the Plea Agreements in the sole discretion of the Offices.

The General Counsels of the Parents, Jane Langford and Cynthia Adams, are duly authorized by the Boards of Directors of the Parents to sign this Certification on behalf of the Boards of Directors.

By: Jane Langford
Jane Langford
Toronto-Dominion Bank,
d/b/a "TD Bank Group"

Dated: October 9 / 24

By: Cynthia Adams
Cynthia Adams
TD Group US Holdings LLC

Dated: 10-9-24