UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:	**)**	
	)	**Number 2024-02**
TD Bank, N.A. and TD Bank USA, N.A.	**)**	
	)	

CONSENT ORDER IMPOSING CIVIL MONEY PENALTY

The Financial Crimes Enforcement Network (FinCEN) conducted a civil enforcement investigation and determined grounds exist to impose a Civil Money Penalty against TD Bank, N.A. and TD Bank USA, N.A. (collectively, TD Bank or the Bank)[1] for violations of the Bank Secrecy Act (BSA) and its implementing regulations.[2] TD Bank admits only to the facts admitted in the October 10, 2024 plea agreements between T.D. Bank, N.A. and TD Bank US Holding Company and the U.S. Department of Justice (DOJ) and neither admits nor denies the remainder of the facts set forth herein, consents to the issuance of this Consent Order, agrees to pay the civil money penalty imposed in this Consent Order, and agrees to comply with the provisions of this Consent Order, including, but not limited to, the Undertakings.

[1] References to TD Bank or the Bank herein refer collectively to TD Bank, N.A. and TD Bank USA, N.A., not to the TD Bank Group or The Toronto-Dominion Bank. For part of the Relevant Time Period, the Bank's BSA Officer reported to TD Bank US Holding Company's board of directors as well as the audit committee thereof (as well as the Global Head of AML). References to the board of directors are to TD Bank's board (the Bank's Board) or its parent TD Bank US Holding Company's board (U.S. Parent Board), unless expressly stated otherwise (collectively, the Boards). Similarly, references to executives are to employees of TD Bank unless stated otherwise.

[2] The BSA is codified at 12 U.S.C. §§ 1829b, 1951-1960, 31 U.S.C. §§ 5311-5314, 5316-5336 and includes other authorities reflected in notes thereto. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.

I. JURISDICTION

Overall authority for enforcement and compliance with the BSA lies with the Director of FinCEN, and the Director of FinCEN may impose civil penalties for violations of the BSA and its implementing regulations.[3]

At all times relevant to this Consent Order, TD Bank was a "bank" and a "domestic financial institution" as defined by the BSA and its implementing regulations.[4] As such, TD Bank was required to comply with applicable BSA regulations.

II. STATEMENT OF FACTS

The conduct described below took place from at least 2012 through May 9, 2024 (the Relevant Time Period) unless otherwise indicated.

A. FinCEN

FinCEN is a bureau within the U.S. Department of the Treasury and is the federal authority that enforces the BSA by investigating and imposing civil money penalties on financial institutions and individuals for willful violations of the BSA.[5] As delegated by the Secretary of the Treasury, FinCEN has "authority for the imposition of civil penalties" and "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies

[3] 31 U.S.C. § 5321(a); 31 C.F.R. § 1010.810(a), (d); *see* U.S. Department of the Treasury, Treasury Order 180-01 (Jan. 14, 2020).

[4] 31 U.S.C. § 5312(a)(2), (b)(1); 31 C.F.R. § 1010.100(d), (t)(1).

[5] 31 U.S.C. § 5321(a). In civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose. TD Bank admits to "willfulness" only as the term is used in civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1).

exercising delegated authority under this chapter," including the Office of the Comptroller of the Currency (OCC).[6]

B. OCC

The OCC is a federal banking agency within the U.S. Department of the Treasury that has both delegated authority from FinCEN for examinations and separate authority under Title 12 of the United States Code for compliance and enforcement.[7] Under this authority, the OCC conducts regular examinations and issues reports assessing a bank's compliance with the BSA and other requirements.

C. TD Bank, N.A. and TD Bank USA, N.A.

TD Bank is an interstate federally chartered bank headquartered in Cherry Hill, New Jersey. The Bank is a member of TD Bank Group and is an indirect, U.S. subsidiary of The Toronto-Dominion Bank of Toronto, Canada, a global systemically important bank[8] whose shares are dually listed and traded on both the New York and Toronto Stock Exchanges under the ticker symbol "TD."

The Bank employs approximately 27,000 personnel and maintains over 1,100 branches and over 2,500 ATM locations in 15 states and the District of Columbia. The Bank's most recent annual financial disclosure, for the year ending on December 31, 2023, reported net income of approximately $2.3 billion and its total assets at approximately $367 billion. TD Bank is the 10th largest bank by assets in the U.S.

---

[6] 31 C.F.R. § 1010.810(a), (d).

[7] *Id.*; 12 U.S.C. § 1818(s)(2), (s)(3); 12 C.F.R. § 21.21.

[8] The Financial Stability Board (FSB), in consultation with Basel Committee on Banking Supervision (BCBS) and national authorities, annually identifies a list of global systemically important banks. This process considers a range of indicators of a financial institution's systemic importance focused on cross-border connections and global, negative externalities. *See* FSB, 2023 List of Global Systemically Important Banks (G-SIBs) (Nov. 27, 2023).

1. FinCEN's 2013 Consent Order with TD Bank

On September 22, 2013, FinCEN issued a Civil Money Penalty to TD Bank related to failures to file suspicious activity reports (SARs) associated with its involvement in the Scott Rothstein Ponzi scheme.[9] The OCC brought a parallel enforcement action for the same conduct. TD Bank facilitated transactions related to the Rothstein Ponzi scheme from April 2008 through October 2009 and failed to identify and report suspicious activity.[10] FinCEN determined that this failure resulted from, among other deficiencies, insufficient training of TD Bank's business and anti-money laundering (AML) staff. This lack of training included failures to appropriately understand Ponzi schemes and their activity and identify suspicious activity.

D. Bank Secrecy Act Requirements

AML Program: The BSA and its implementing regulations require U.S. banks, such as TD Bank, to implement and maintain an AML program, including policies, procedures, and controls to assure ongoing compliance with the applicable provisions of the Bank Secrecy Act.[11] TD Bank is also required to: (i) conduct independent testing for compliance; (ii) designate an individual or individuals responsible for implementing and monitoring the operations and internal controls of the program; (iii) conduct ongoing training for appropriate persons; and (iv) implement appropriate risk-

[9] FinCEN, In the Matter of TD Bank, N.A., Number 2013-1 (Sept. 22, 2013).

[10] More recently, TD Bank processed transactions related to another large Ponzi scheme. From 2018 to 2023, the Bank processed over 3,000 transactions with an aggregate value of more than $300 million. Investors were defrauded through investments into a purported real estate company. TD Bank only began filing SARs on this activity after receiving a law enforcement inquiry in 2021, and this reporting covered only approximately 1% of the suspicious activity that TD Bank processed related to this scheme. In 2024, more than six years after the activity began, the Bank filed a SAR on approximately 98% of these transactions. Of more than 3,000 suspicious transactions, nearly half were effected via checks and check deposits—over $40 million—that TD Bank was not properly monitoring, as the Bank did not monitor checks. *See infra* Section II.E.2.a.1.

[11] 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210.

based procedures for conducting ongoing customer due diligence, including, but not limited to, (a) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and (b) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[12]

Reporting Obligations – Currency Transaction Reports (CTRs): The BSA and its implementing regulations impose an obligation on banks to file a report of 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, including multiple transactions that aggregate to more than $10,000.[13] A bank must file a CTR within 15 days after the transaction is conducted.[14] Accurate, complete, and timely CTRs are critical to the utility of BSA data in combating financial crimes, terrorist financing, and other illicit activity. Additionally, a bank needs to verify and record the name and address of the individual presenting a transaction.[15]

Reporting Obligations – SARs: A bank must identify suspicious transactions relevant to a possible violation of law or regulation in SARs filed with FinCEN.[16] Specifically, the BSA and its implementing regulations require banks to report transactions that involve or aggregate to at least $5,000, are conducted or attempted by, at, or through the bank, and that the bank "knows, suspects,

[12] 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210(a). These are often referred to as the five "pillars" of a bank's AML program.

[13] 31 U.S.C. § 5313; 31 C.F.R. § 1010.311 (banks "shall file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, though, or to such financial institution which involves a transaction in currency of more than $10,000"); *see also* 31 C.F.R. §§ 1010.310, 1010.313(b).

[14] 31 C.F.R. § 1020.310; 31 C.F.R. § 1010.306(a)(1).

[15] 31 C.F.R. § 1010.312.

[16] 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320.

or has reason to suspect" are suspicious.[17] A transaction is "suspicious" if a bank "knows, suspects, or has reason to suspect" that the transaction: (i) involves funds derived from illegal activities, or is conducted to disguise funds derived from illegal activities; (ii) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations implementing it; or (iii) has no business or apparent lawful purpose or is not the sort in which the customer normally would be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction.[18] A bank is generally required to file a SAR no later than 30 calendar days after the initial detection by the bank of the facts that may constitute a basis for filing a SAR.[19]

The reporting and transparency that financial institutions provide through these reports is essential financial intelligence that FinCEN, law enforcement, and others use to safeguard the U.S. financial system and combat serious threats, including money laundering, terrorist financing, organized crime, corruption, drug trafficking, and massive fraud schemes targeting the U.S. government, businesses, and individuals.[20]

E. TD Bank Failed to Implement and Maintain an AML Program

Despite awareness of significant deficiencies, the Bank willfully failed to implement an AML program that met the BSA requirements during the Relevant Time Period. The failures, described in the subsections below, spanned all pillars of TD Bank's AML program. Although the violations involved a host of unique issues, these violations demonstrate key and systemic

[17] *Id.*

[18] 31 C.F.R. § 1020.320(a)(2).

[19] 31 C.F.R. § 1020.320(b)(3).

[20] FinCEN, FIN-2014-A007, FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance (Aug. 11, 2014).

failures by TD Bank, including awareness of certain issues by senior management, as described below.

TD Bank willfully failed to establish an adequate AML program. The Bank did not invest sufficient time, money, or managerial resources in the creation and maintenance of TD Bank's AML program, nor did the Bank take sufficient steps to ensure TD Bank's ongoing compliance with the BSA. As described more fully below, TD Bank failed to devote sufficient resources to BSA compliance, and refused to invest in improvements to address such gaps when they were deemed too costly, thus allowing illicit activity to flow through the Bank.[21] TD Bank vastly underinvested in its AML compliance efforts, with TD Bank knowingly spending an order of magnitude less than its peers. Additionally, the Bank's AML staffing was not proportionate to its size, risk profile, and ongoing compliance concerns: during the periods of TD Bank's most acute issues (including those related to backlogs from insufficient staffing), AML spending remained flat. As explained below, when a host of significant AML compliance issues arose during the Relevant Time Period, the Bank consistently chose to address them in the least costly way possible, even if it meant ignoring failures and refusing to meaningfully remediate issues and prevent recurrences.

The systemic failures of TD Bank's AML program caused actual and material harm to the U.S. financial system. As set forth below, during the Relevant Time Period, funds flowing through TD Bank have been linked to numerous prosecutions, some of which included TD Bank personnel, for various financial crimes that likely could have been prevented, mitigated, or at least timely reported, if TD Bank implemented and maintained an adequate AML program.

[21] *Id.* ("For the [AML] program to be effective, the institution should devote appropriate support staff to its BSA/AML compliance program based on its risk profile. The failure of an institution's leaders to devote sufficient staff to the BSA/AML compliance function may lead to other failures.").

The Bank's inattention to, and underinvestment in, its AML program, including the failures of its AML management, led to willful failures during the Relevant Time Period across each pillar of its AML program: (i) ineffective oversight and management of TD Bank's compliance obligations by the individual—its BSA Officer—responsible for coordinating and monitoring the Bank's day-to-day compliance with the BSA, including the BSA Officer's failure to timely and properly escalate material issues and failures by the Bank's Board to provide adequate resources for the BSA Officer to discharge their duty of assuring the Bank's compliance with the BSA; (ii) inadequate internal controls, most notably failure to ensure appropriate transaction monitoring; (iii) failure to properly train its staff on AML typologies and risks the Bank knew were associated with the products and services the Bank offered; (iv) deficient risk-based customer due diligence, including missing blatant disparities between customers' actual activity and what would reasonably be expected based on available information; and (v) insufficient independent testing that failed to reasonably identify material gaps.

1. Failures Related to the Designated Individual Responsible for Coordinating and Monitoring Day-to-Day Compliance[22]

TD Bank was required to designate an individual to be responsible for coordinating and monitoring the Bank's day-to-day compliance with the BSA—a "BSA Officer." Longstanding regulatory guidance has made clear that this requirement is central to the effective function of a bank's AML program and that the mere act of appointing an individual to the role of BSA Officer is

[22] Unless otherwise indicated, references to TD Bank's BSA Officer refer to the individual who held this position from May 2019 to May 2023, when they were removed from the role by the Bank. During this time, the BSA Officer reported to the U.S. Parent Board, the audit committee thereof, and the Global Head of AML. Prior to assuming the BSA Officer role, this individual served as the head of the Bank's AML Investigations Unit (AIU).

insufficient to assure and monitor the bank's compliance with the BSA;[23] thus, the existence of an individual with this title in a bank does not alone fulfill this requirement. To have an effective AML program, a bank's board of directors must ensure that the designated BSA Officer has appropriate authority, independence, and access to resources to administer an adequate BSA compliance program.[24]

As detailed below, TD Bank's BSA Program was non-compliant for the following reasons: (i) its BSA Officer and AML management failed to seek, and TD Bank otherwise failed to allocate, sufficient resources across budget, personnel, and technology; (ii) it had a siloed governance structure that resulted in the designated BSA Officer lacking sufficient control or accountability for the Bank's AML program;[25] and (iii) there was a lack of oversight over the Bank's high-risk operations and gaps described below for which the BSA Officer failed to take accountability, including the BSA Officer's awareness of material gaps in the Bank's transaction monitoring system that went unabated for many years.[26]

a) Failure to Ensure Sufficient Staffing and Resources to the BSA Officer

TD Bank willfully failed to establish or maintain an adequate AML program, in part, by failing to provide sufficient resources and staffing to the Bank's AML program, and thus preventing the BSA

[23] *See* FinCEN, FIN-2014-A007, FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance (Aug. 11, 2014).

[24] *Id.*

[25] The Bank's Canadian parent, Toronto-Dominion Bank, maintains a Global Chief AML Officer (Global Head of AML), who oversees both the Canadian parent bank and the U.S. subsidiary banks. With respect to the U.S. subsidiary banks, the BSA/AML obligations were managed by the BSA Officer, who reported to both the Chief Risk Officer of the Bank in the U.S. and the Global Head of AML in Canada. This reporting structure led to complications; many AML senior managers with BSA responsibilities, most notably an AML Technology head and head of AML Operations, only reported to the BSA officer via a "dotted line" and reported directly to the Global Head of AML at the Canadian parent. Furthermore, the BSA Officer delegated management and oversight of critical functions within the Bank's AML program (*e.g.*, transaction monitoring) to these individuals.

[26] *See infra* Section II.E.2.a.

Officer from performing their duties effectively. For example, TD Bank's compensation system reflected the apparent disincentive for the BSA Officer to incur costs needed to assure the Bank's compliance with the BSA. At times during the Relevant Time Period, both the Global Head of AML and the BSA Officer's annual self-assessments noted as an "accomplishment" their respective abilities to "develop [the AML] program within a flat cost paradigm without compromising risk appetite." AML management did not timely escalate requests for additional resources to executive management or the Boards, although the U.S. Parent Board was made aware that "inadequate staffing levels" were a root cause of issues that persisted during the Relevant Time Period. When confronted with the reality that TD Bank's pennywise, pound-foolish approach caused the Bank to violate the BSA, the Bank refused to make the requisite investments to prevent future violations until near the end of the Relevant Time Period, after the investigations resulting in this Consent Order and parallel resolutions were underway. At that time, and under the direction of the Boards, the Bank began a large-scale remediation effort that included replacing the BSA Officer, as well as increasing AML staffing, updating and redelivering training programs, and enhancing policies and procedures.

TD Bank's severe understaffing persisted throughout the Relevant Time Period. From 2017 to 2019, the compound annual growth rate of TD Bank's assets—and, as explained below, due to persistent gaps in its program, corresponding measures of AML risk—significantly exceeded the Bank's spending on AML compliance, which remained roughly flat. During certain earnings calls in this period, TD Bank Group management commented favorably about its operating leverage (which is defined as the difference between growth in revenues and growth in expenses) and noted that "expenses have been relatively stable."[27]

[27] *See, e.g.*, TD Bank Group, Q1 2018 Earnings Conference Call (Mar. 1, 2018) ("Turning to the U.S., our U.S. Retail Bank . . . delivered over 400 basis points of operating leverage."); TD Bank Group, Q4 2019 Earnings Conference Call (Dec. 5, 2018).

TD Bank only began to use a "forecast model" in which AML resourcing needs were projected in advance of an upcoming quarter starting in late 2019 and increased hiring in 2020. However, in 2022, the AML headcount decreased to ***less than*** 2020 totals, while the number of transaction monitoring alerts of potentially suspicious transactions continued to rise. Only once the Bank came under regulatory scrutiny were the relevant issues escalated and given sufficient attention by the Boards and TD Bank Group, with the Bank materially increasing AML resources and nearly doubling its AML staff over a six-month period ending in May 2024.

The effects of the Bank's persistent under-resourcing and understaffing reverberated throughout every aspect of its AML program, but were especially apparent in the extensive, persistent, and prolonged backlogs within the AML function throughout much of the Relevant Time Period. As described below, these resource-related backlogs manifested themselves in two main areas within TD Bank's AML program: (i) backlogs of alerts requiring review by investigators to resolve, and, where appropriate, prepare a SAR for reporting to FinCEN, and (ii) backlogs of customers to be exited that the Bank had determined presented unacceptable AML risk. In each case, the Bank had opportunities to increase staffing and resolve the backlogs effectively, but took a delayed and insufficient approach to do so.

AML Investigations Unit Backlogs. From 2016 through 2019, TD Bank faced extensive backlogs in the Detection and Further Investigation queues within its Financial Intelligence Unit (AML Investigations Unit, "AIU"), which reviewed alerts and case investigations linked to potentially suspicious activity to determine if the Bank needed to file a SAR with FinCEN and/or take other mitigating actions, that were attributable to understaffing. During this time, reporting by the BSA Officer to the Boards and the AML Oversight Committee consistently showed the AIU Detection and Further Investigations teams in "red" status, indicating significant backlogs.

In 2016, the then-head of the AIU (who subsequently became the Bank's BSA Officer) delivered a presentation to AML senior management about resources, reporting that the AIU was understaffed by more than a dozen full-time employees. However, despite self-identifying the need for additional resources, the head of the AIU recommended waiting to reassess the need to hire new employees to fill this gap and extending the contracts of temporary employees in the meantime. In September 2017, this individual delivered another memo, addressed to the Global Head of AML, seeking approval to pay overtime to work through other, related backlogs involving high-risk customers caused by staffing that was not commensurate with the volume of cases to be completed. The memo anticipated a return to "green" status before the end of 2017. Permission for overtime was granted, but the backlog and related resourcing issues persisted.

A subsequent action plan submitted to internal audit in June 2018 identified the backlog's root cause as inadequate staffing levels, as well as transaction monitoring system issues. In 2018, the AML program registered ***over 70,000 backlogged detection alerts*** and ***roughly 3,000 aged subpoena responses and further investigation cases***, with less than 60% of alerts falling within benchmarks for timely detection. An AML manager of the PEP investigations team also cited resourcing constraints during this portion of the Relevant Time Period: in 2018, this manager noted that the Bank simply "won't hire [additional staff] for us," and in 2019 this manager noted that no response was received on open requests for additional staffing going back several quarters.

By 2019, the detection and subpoena processing case queues had not decreased, and a senior executive suggested the program was not "adequately resourced/managed," a situation they described as "really concerning." The Bank's Global Head of AML's response to the senior executive—to whom they reported—was, in part, to "identify opportunities to scale back review or investigative

rigor" and reduce analyst time to investigate potentially suspicious activity, without reasonably addressing the ongoing problem.

The Bank engaged contractors in 2018 to help "***gradually reduce***" these backlogs, but nonetheless failed to investigate thousands of alerts for almost a year. In 2020, the AIU backlog was finally in "green" status from belated increases in full-time staffing, as well as other changes, such as offering overtime and other process improvements. In addition to these other measures, the Bank continued to rely in part on contractors despite reports from AML employees that the contractors delivered "sub-par, shoddy, and incompetent work that has created even more confusion" for full time employees.

In sum, for several years, the BSA Officer presented overly optimistic expectations to other AML senior management and to the U.S. Parent Board that the backlogs would be alleviated, even as the Bank continued to miss internal deadlines and failed to make meaningful investments in resources to address them. The U.S. Parent Board was informed about the issue, but did not act in a timely manner, despite mounting evidence that the issues were not resolving over the years.

Demarketing Backlogs. Although the Bank eventually made progress on the AIU backlogs, these strides contributed to backlogs involving or related to the Bank's procedures for assessing and determining when the Bank elects to close a customer account.[28] TD Bank did not have a process to apply restrictions or appropriate mitigating controls to customers that are the subject of SAR filings. Instead, the Bank left demarketing adjudication to an investigator after a certain number of SAR

[28] Although banks are permitted to establish the policies, procedures, and controls that they believe will allow them to comply with the BSA, such policies, procedures, and controls must be supported by appropriate resources (which TD Bank failed to do, including its demarketing processes). Moreover, FinCEN encourages banks to consider a range of approaches in mitigating identified risks—while closure of accounts engaged in suspicious activity may be appropriate in a number of circumstances, in others, a bank may be able to effectively mitigate risk through enhanced monitoring, restrictions on products or services, or other steps short of account closure.

filings. As the Bank's AIU began working through its large queue of potentially suspicious transactions, inevitably a portion would be found to be suspicious, and some of the related customers would be subject to the Bank's demarketing processes. TD Bank's lack of staffing and backlogs allowed these customers—which the Bank deemed to pose an unacceptable money laundering risk—to continue transacting without appropriate controls consistent with the Bank's own AML program.

From 2018 to 2021, customers waiting to be demarketed ***received*** more than $5 billion into their accounts, with an average of more than $250,000 per account ***after*** a request to initiate account closure by an AML employee. For example, in late 2018, the Bank identified an Ecuador-based brokerage firm registered to a Miami residence as conducting over $200 million in suspicious foreign activity, which the AIU requested to close in October 2018. The Bank, however, did not close the accounts for almost a year after the initial request to close by relevant AIU personnel and allowed the entity to continue to transact without restriction until its July 2019 closure, despite filing SARs on the customer before and during the prolonged demarketing period.

In 2018, nearly 1,000 demarketing requests aged beyond the 35 days TD Bank's AML policy allowed for the review and processing of such requests. Prior to approximately the summer of 2019, only one member of the relevant team was responsible for reviewing requests to close retail accounts, leading to delays in decisioning requests that frequently exceeded two weeks, and TD Bank generally taking more than two months to notify an account closure to the associated retail branch. Despite the demarketing queue reporting "green" within 2019, resource constraints continued later that year.[29]

In February 2020, the demarketing queue again returned to "green" status as additional temporary resources joined the demarketing team to review the previous backlog, but again quickly

[29] In early 2019, account closure requests increased 62.5%, stemming from AIU referrals as the AIU's backlog started to resolve.

fell into another backlog. From March through May 2020, as a result of the COVID-19 pandemic, the Bank implemented a decision to pause certain portions of the demarketing process. The Head of AML Operations sent a memo to AML senior management, including the BSA Officer, warning that, following the COVID-19 pause on demarketing through May 2020, the AIU "demarketing, and advisory teams could fall into a backlog," but only four employees were staffed to resolve these cases. As a result, demarketing backlogs persisted through mid-2021, when the Bank finally allocated additional resources to properly implement its demarketing policies.

b) Siloed Governance Structure

The Bank's AML governance structure also impaired the BSA Officer from effectively managing the Bank's compliance with the BSA. For example, the BSA Officer lacked direct authority over an AML Technology Head, who oversaw the transaction monitoring system, as well as the head of AML Operations within the AML function. As explained in Section II.E.2 below, this governance structure was especially problematic given the severe and widespread issues TD Bank experienced with its transaction monitoring software during the Relevant Time Period.[30] An AML Technology Head reported directly to the Global AML Officer for the U.S. and Canada, with only "dotted line" reporting to the BSA Officer. This structure led to TD Bank's BSA Officer not being accountable for the numerous and persistent control gaps in an integral component of the Bank's AML program: core functions, such as scenario development within the transaction monitoring system, were not subject to direct oversight by the BSA Officer. There is no evidence that the BSA Officer ever raised a concern about this structure to the Boards. The BSA Officer improperly relied on one of their direct reports for approval of changes to transaction monitoring scenarios and generally did not review such approvals.

[30] *See infra* Section II.E.2.

c) Lack of Effective Oversight of High-Risk Operations

Finally, TD Bank's BSA Officer and AML senior management who reported to the BSA Officer failed to effectively monitor the Bank for day-to-day compliance with the BSA—especially considering the elevated risk of money laundering or terrorist financing present in certain aspects of the Bank's operations.[31]

The Bank's cash operations also suffered from deficient monitoring of high-risk transactions. Compared to peers, TD Bank engaged in cash processes that created higher risk for the Bank to be used as a vehicle to facilitate illicit activity. For example, until April 2021, the Bank permitted customers to go to a branch and exchange cash for an official bank check without first depositing the cash into the customer's account, resulting in the transaction not being reflected in the customer's account statements. Furthermore, limitations in the transaction monitoring scenarios applicable to this activity led to ineffective monitoring for potentially suspicious activity. The Bank produced internal reports highlighting which customers—and the branches at which they transacted—generated the greatest amount of cash activity in a given period. These manual reports were not reviewed and were not designed to mitigate AML risks, and therefore did not serve as an effective control.

In 2020, these reports of the greatest amount of cash activity identified a New York-area company purporting to operate in the clothing industry as among the Bank's top customers for cash transactions, with this customer conducting $8 million to $20 million each quarter over hundreds of transactions across multiple TD Bank branches. This included a period during the COVID-19

[31] The BSA Officer reported to the Boards that the AML function had a responsibility to maintain an appropriate framework to identify and monitor emerging and evolving risk and provided the Boards with examples of such risk and certain corresponding actions that the AML function had taken.

pandemic when many cash-intensive businesses experienced declines in transaction volumes. DOJ later indicted an individual associated with the customer, Da Ying Sze (Sze), for his part in a larger conspiracy to operate as an unlicensed Money Services Business (the Sze Network).[32] The BSA Officer's only comment on the report during this portion of the Relevant Time Period involved a request that the report be generated less frequently, changing from a monthly report to a quarterly report, purportedly in order to gain more insight on trends (although there is no evidence that such trends were ever identified). Further, the BSA Officer, as well as people involved in the generation of these reports to the BSA Officer, never questioned why a clothing company would be engaged in such a high level of cash activity volume during the pandemic, even though an AML analyst specifically highlighted this customer in the report. No steps were taken to verify that these reports were reviewed.

Appointing multiple AML managers without any prior experience in AML also hindered the BSA Officer's ability to effectively monitor the Bank's day-to-day compliance with the BSA. In particular, the heads of the AIU and AML Operations for portions of the Relevant Time Period oversaw critical AML processes without ***any*** previous AML experience. The appointment of AML managers without sufficient AML knowledge directly conflicts with U.S. BSA/AML regulatory guidance on assuring and monitoring the Bank's compliance with the BSA, which requires suitable resources, including staff, who maintain the proper skills and expertise necessary to support the timely identification, monitoring, reporting, and management of a bank's illicit financial activity risks.[33]

[32] For further discussion on the Sze network, *see infra* Section II.E.3.b.

[33] FinCEN, FIN-2014-A007, FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance (Aug. 11, 2014).

The BSA Officer further failed to monitor the Bank's day-to-day BSA compliance related to the involvement of Bank personnel in suspicious activity. Specifically, internal reporting to AML senior management neither highlighted emerging patterns and trends of concern nor conveyed the significance of an insider's involvement in suspicious activity.[34] This contributed to the Bank's failure to timely detect related and, in several cases, ongoing employee misconduct.[35] In some cases, the Bank only looked into such activity after law enforcement arrested or charged the relevant employees.[36]

As detailed below, the BSA Officer also drastically scaled back recommendations in a report to AML senior management on funnel account activity being effected through the Bank.[37] Specifically, AML compliance personnel initially provided the following recommendations in a draft briefing to AML senior management: (i) focus training and fine-tune customer identification protocols; (ii) "dig deeper for more individuals;" and (iii) "reconsider cash deposit policies." The BSA Officer instructed the AML compliance personnel to remove the foregoing suggestions.

At times, the Bank also experienced challenges with reporting information to AML senior management. In one instance, the AIU reported that it temporarily could not provide accurate volumes and reporting due its ongoing technology issues. The AIU acknowledged that the Bank had "issues with accurately reporting volumes."

[34] *See infra* Section II.G.4 and Section II.G.6. The Bank failed to identify potential illicit activity by its own employees, which resulted in embezzlement from customer accounts, Paycheck Protection Program (PPP) loan fraud, and facilitating money laundering.

[35] *See infra* Section II.G.4 and Section II.G.6.

[36] There are some examples where the Bank detected the activity and reported it to law enforcement.

[37] *See infra* Section II.E.2.a. The Bank's failure to timely adopt these recommendations contributed to the funnel account activity persisting without appropriate controls for an extended period of time.

2. Inadequate Policies, Procedures, and Internal Controls

Throughout the Relevant Time Period, TD Bank failed to address significant gaps and other deficiencies in its process to identify and report suspicious transactions. For most of the Relevant Time Period, and consistent with the Bank's other piecemeal approaches to AML compliance, TD Bank failed to adopt a holistic approach to money laundering, terrorist financing, or other illicit finance risks assessments into its process for identifying and reporting suspicious activity. During the transaction monitoring system's initial implementation in 2008, TD Bank applied certain "off-the-shelf" scenarios provided by its vendor without consideration as to whether such scenarios needed to be tailored for the products and services TD Bank offered or whether they were sufficient to the specific risks the Bank faced.[38] Ultimately, the system's coverage excluded large swaths of the Bank's transactions: in 2023 alone, the coverage gaps applied to ***several trillion dollars*** of transactions that were not screened by the Bank's transaction monitoring system. As detailed below, the BSA Officer was aware of at least one of these gaps involving checks in at least 2017, and other AML senior management became aware of additional, more extensive gaps later in the Relevant Time Period; with limited exceptions, they took no action to escalate them, nor did they inform FinCEN or any of the Bank's other AML supervisors of the nature and extent of the gaps.

As detailed in each of the subsections below, over an extended period of time, TD Bank failed to reasonably respond to significant issues with its ability to fulfill its obligation to identify and report suspicious activity. TD Bank's failure to invest in technology and staffing necessary to implement its program, which required a functioning transaction monitoring system, led to failures to identify

[38] Within a few years of implementing its transaction monitoring system in 2008, TD Bank identified deficiencies with the system's coverage. Subsequent external reviews found the transaction monitoring system was not subject to comprehensive scenario reviews and failed to provide adequate coverage across all transaction types. From 2013 to 2015, TD Bank implemented a dozen new scenarios covering terrorist financing, foreign currency transactions, cross border activity in high-risk countries, and transactions in sanctioned countries. The belated implementation of these fundamental scenarios demonstrates the Bank's haphazard approach and resulting risks.

and timely report money laundering activity. TD Bank's governance of its transaction monitoring system also proved ineffective, as Bank leadership allowed temporarily "paused" scenarios to remain dormant for years and failed to implement new scenarios even after identifying risks. Finally, the Bank also did not effectively test its transaction monitoring system to ensure that it captured the Bank's risks comprehensively. There is no evidence, until late in the Relevant Time Period, that any of this was escalated to executive management or the Boards.

a) TD Bank's Approach to Transaction Monitoring Was Willfully Deficient and Created Significant Gaps in Reporting Suspicious Activity

TD Bank failed to make meaningful changes to its transaction monitoring scenario coverage during much of the Relevant Time Period. This deficient approach persisted despite recommendations by Bank personnel to add new scenarios and modify existing scenarios so the Bank could properly identify and report suspicious transactions. TD Bank attributed the torpor in its transaction monitoring system to technology issues, but the root causes were the Bank's severe underinvestment in AML compliance combined with a flawed and piecemeal approach to addressing issues plaguing the transaction monitoring system.

Transaction Monitoring System Upgrade. Beginning in late 2016 and persisting through the end of 2019, TD Bank attempted to upgrade to a more recent version of the transaction monitoring software. The Bank viewed this as an important update needed to address several significant issues and limitations associated with its transaction monitoring software. The upgraded system would allow for more customized rules, which could have supplemented manual monitoring that, before the upgrade commenced, helped cover nearly half of the typologies the Bank identified as relevant risks. TD Bank's inadequate transaction monitoring system also obstructed the Bank from implementing "customer segmentation" capabilities, which would have provided the Bank with a risk-based

approach to reviewing customer transactions. Initially, TD Bank estimated this upgrade would be completed by October 2017.

However, due to a combination of insufficient resources—including personnel and technology funding, technological issues, and ineffective planning by AML management—the project quickly fell behind schedule.[39] During this upgrade, the Bank also paused all changes to transaction monitoring scenarios. From 2017 to 2019, numerous reports about the project to AML senior management and the U.S. Parent Board identified that it was not on target, yet the Bank failed to take action. For example, in 2018 the BSA Officer reported to the AML Oversight Committee that the status of the upgrade was "yellow due to overspent approved funding," thus suggesting the need for additional resources to complete the project. The resourcing issues continued to persist and the upgrade was further delayed. In 2019, the BSA officer presented to the Audit Committee an AML Technology Portfolio Readiness Assessment, which found that given a "reliance on a limited pool of people, leadership, and infrastructure to support the full portfolio of work" at the Bank, there was a "lack of sufficiently dedicated and capable resources across all streams of work" as well as a "historical siloed portfolio management approach." A 2019 budget discussion indicated the Bank had been spending more on staffing to "avoid adding to the backlog" of alerts for investigation, which stemmed in part from the transaction monitoring system's technological failures. The transaction monitoring system upgrade was not fully implemented until December 2019.

Transaction Monitoring System Replacement. In late 2019, TD Bank decided to consider changing vendors for its transaction monitoring system but did not select the successor system until

[39] For example, a 2017 presentation to the Executive Steering Committee on TD Bank's transaction monitoring system upgrade stated discussions were required on necessary resourcing within technology, and a business case was preemptively updated to include an anticipated cost avoidance request from the Bank's finance department. Similarly, a request for increased memory during the upgrade was also rejected due to costs. In December 2017 the Bank dedicated additional funding to the upgrade.

early 2021. While transitioning to this new transaction monitoring system, TD Bank again paused changes to scenarios. The new transaction monitoring system only began a phased implementation in August 2024, and will continue to roll out in phases extending into 2025. After the Bank decided on and began the transition to a new system, it limited changes to its existing transaction monitoring system, including not adding any new scenarios, for four years.

As detailed below, these two largely co-extensive portions of the Relevant Time Period resulted in the Bank's willful failures to address critical gaps in its ability to identify and report suspicious activity to FinCEN.

(1) Domestic Transaction Monitoring

TD Bank failed to monitor a number of transaction types, including ACH,[40] certain funds transfers,[41] and certain monetary instruments[42] (including remote deposit capture (RDC)).[43] This

[40] ACH, or Automated Clearing House, transactions are transfers of funds up to $1 million that use the ACH network to move money from one U.S. bank or credit union to another financial institution. Although ACH transactions can be sent outside the United States, the bulk of the transfers are domestic in nature and range from automatic bill payments and payroll/direct deposits of wages and government benefits to, more recently, certain popular peer-to-peer payment applications, such as Venmo. TD Bank's monitoring system lacked transaction codes necessary to monitor 98% of domestic ACH transactions.

[41] Funds transfers are transactions by which funds move from one institution to another, or one account to another, at the direction of an institution's customer and through the transmission of electronic instruction messages that cause the institutions to make the required bookkeeping entries and make the funds available to the beneficiary. Roughly half of TD Bank's fund transfers went unmonitored and included international debit card purchases.

[42] Monetary Instruments include: (i) coin or currency of the United States or of any other country; (ii) traveler's checks in any form; (iii) negotiable instruments (including checks, promissory notes, and money orders) in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; (iv) incomplete instruments (including checks, promissory notes, and money orders) that are signed but on which the name of the payee has been omitted; and (v) securities or stock in bearer form or otherwise in such form that title thereto passes upon delivery. The Bank failed to monitor nearly all monetary instruments.

[43] TD Bank considered RDC to be a subset of monetary instrument transactions. RDC transactions represent a bank's acceptance of checks for deposit using electronic images instead of the original, physical, paper versions of the checks, such as through a check deposit feature within a bank's mobile application. Longstanding regulatory guidance has demonstrated the need for banks offering RDC as a delivery system to properly assess the extent to which RDC transactions could implicate their ability to comply with BSA obligations, including suspicious activity monitoring. FFIEC, Risk Management of Remote Deposit Capture (Jan. 14, 2009). The Bank knew since 2011 it lacked specific transaction codes and scenarios necessary to monitor RDC transactions.

failure to monitor represented over 80% of the activity in these types of transactions and aggregated to ***trillions of dollars in value***. The coverage gaps occurred throughout the Relevant Time Period.

Since at least 2012, TD Bank knew it failed to monitor virtually ***any*** domestic ACH transactions. In 2012, AML employees recognized a need to do so and proposed a scenario to monitor such ACH transactions. An AML senior manager rejected their request.

A 2017 internal coverage assessment of the Bank's transaction monitoring system reported "no active ACH monitoring" was in place for domestic ACH transactions. The review and approval of these annual coverage assessments, that determined the Bank was not monitoring this significant category of transactions, was delegated by the BSA Officer to subordinates.

Subsequent coverage assessments incorrectly reported that the transaction monitoring system covered ACH payments, even though such coverage was limited to international ACH transactions only (a small portion of the total population of ACH transactions). This inaccurate reporting continued for the remainder of the Relevant Time Period because the Bank never conducted any mapping or testing to verify which types of transactions were covered by the transaction monitoring system.[44]

Once these substantial gaps were identified by one of TD Bank's regulators, the Bank reported incorrectly that its risk assessment historically categorized ACH payments as low risk, which the Bank claimed justified the lack of monitoring for these transactions. However, the Bank later determined that it could not identify any "historic documentation related to risk analysis or risk

[44] The Bank conducted periodic coverage assessments during the Relevant Time Period. However, these assessments lacked depth or detail when it came to the Bank's risk rating of certain products. For example, in 2017, TD Bank determined that a set of products that included domestic and international ACH was considered high-risk, but acknowledged no monitoring was in place for domestic ACH transactions, and international ACH transactions were only monitored for a "select list of countries." In 2018, TD Bank reduced the ACH product risk rating to "medium," without any documentation or rationale to support this downgrade. For the remainder of the Relevant Time Period, the Bank maintained the risk rating for ACH as "medium" and failed to perform comprehensive assessments to support its risk rating.

memos related to Domestic ACH risk and its exclusion for monitoring from [the transaction monitoring system]."

TD Bank also failed to properly monitor checks, even though AML senior management knew of this gap and the risks these transactions posed. As early as 2017, the BSA Officer was told the AIU did not "typically monitor for checks," when discussing the AIU's failure to monitor an existing scenario covering rapid movement of funds involving checks. In a 2020 discussion on new scenario recommendations, an AML Compliance manager stated, "[c]urrently we . . . do not monitor checks as far as I have seen, but we see a lot of ML [money laundering] in this space." There is no evidence the BSA Officer escalated the issue to other AML management or the Boards.

TD Bank's failure to conduct appropriate testing and gap assessments of its transaction monitoring system led these monitoring gaps to persist for well over a decade. When TD Bank began transitioning to a new transaction monitoring system, it conducted a mapping exercise; this exercise, though, was not "to make changes to [the existing transaction monitoring system] unless it's a severe gap [because] the scenarios would be addressed in [the new transaction monitoring system]" that, at the time, was over a year out from implementation, which remains ongoing. In connection with this exercise in the summer of 2023, an external consultant alerted the Bank that there would be a significant increase in the number of alerts in the new transaction monitoring system due to, among other factors, additional transactions captured in the new system, including checks and a broader definition for wire payments. An AML senior manager shared with the Global Head of AML that in ***a five and half month test period, the new system would monitor roughly $1 trillion in additional wire transactions than the existing system***.

In August 2023, an AML senior manager responded to the transaction monitoring discrepancies, "WOW, there is a significant difference especially for monetary instruments and

wires!" The Global Head of AML was then informed of the issue and noted the need to understand the "200% increase in wires" that would be captured in the new transaction monitoring system, but failed to escalate the issue to the Boards, other senior management, or its regulators, and failed to implement mitigating controls.

From August 2023 to February 2024, there were at least four presentations to TD Bank executives that compared the coverage between the old and new systems, with each presentation noting a substantial difference between the two, and one describing a ***monthly increase of "$220 billion of transactions (123% increase)"*** covered under the new system's transaction codes. However, during this time, TD Bank executives did not apply mitigating controls or notify regulators. The Bank estimated that it would need to almost triple its AML staff to handle the projected volumes in the future, but did not initiate any remediation efforts. It was only after one of TD Bank's regulators became aware of the gaps that the Bank began taking steps to mitigate the significant ongoing risk that they posed to both the Bank and the broader financial system.

(2) P2P Monitoring

TD Bank's insufficient monitoring included transactions that its customers effected via peer-to-peer (P2P) channels, including Zelle, which the Bank launched for personal accounts in April 2017.[45] Due to the Bank's lack of domestic ACH monitoring, TD Bank did not monitor P2P, such as Venmo or PayPal, if effected through a channel other than Zelle.

[45] "Peer-to-peer transfers allow consumers to make payments to other consumers, usually through a mobile device app. The apps are typically linked to debit or credit card accounts or bank accounts, thereby allowing the funding transfers to proceed through bank-maintained payment networks." *See* Financial Stability Oversight Council, 2019 Annual Report (Dec. 4, 2019).

Non-Zelle P2P. The Bank knowingly failed to appropriately monitor over $100 billion of non-Zelle P2P transactions, such as Venmo transactions, during the Relevant Time Period.[46] Within TD Bank, Non-Zelle P2P transactions were processed as domestic third-party debit card or direct deposit activity in customer accounts. In January 2019, an internal assessment of a terror financing scenario recommended adding coverage for online money transfer systems, such as PayPal, Venmo, and Zelle, to align with FATF guidance.[47] The recommendation stated, "[i]ncluding additional payment types for monitoring within these scenarios may increase the probability of detecting terrorist financing activity as well as reduce any AML risks by not monitoring these transaction types." However, in November 2019, when the Bank was updating its AML transaction codes to allow for changes in its monitoring coverage, the AIU determined that all external P2P vendors, such as Venmo or Square, would be "out of scope." TD Bank never created transaction codes necessary to monitor P2P platforms, instead focusing on creating codes for Zelle only, thereby knowingly excluding these other P2P transactions from any specific scenario monitoring.

As of 2021, when the Bank had ***another*** opportunity to create transaction codes and specific scenarios for P2P transactions, AML senior management improperly concluded the current monitoring mechanism was sufficient. In March 2024, an AML Technology Head's response to

Zelle stands apart from many other P2P applications (such as Venmo) because it is owned and operated by Early Warning Services, LLC, a bank service company owned by seven major U.S. banks; TD Bank is not one of the owners and operators of this company, but TD Bank does allow its customers to use Zelle to effect P2P transactions.

[46] This number includes the following P2P applications: Apple Cash, Block (formerly Square), Cash App, Facebook Pay, Google Pay, Google Wallet, PayPal, and Venmo.

[47] "Some TF cases involving low-value transactions via online payment systems such as PayPal have also been linked to a number of terrorism suspects." *See* Financial Action Task Force, Emerging Terrorist Financing Risks (Oct. 18, 2015).

questions from the Bank's newly hired BSA Officer about monitoring P2P acknowledged that non-Zelle P2P were not "assigned specific tran[saction] codes, [that allow] for systemic monitoring."

Zelle.[48] From 2017 to 2023, about 300 million incoming and outgoing Zelle transactions were conducted at TD Bank with a total value over $75 billion—nearly the same as the total amount of P2P activity that TD Bank customers processed across all other P2P channels combined. Prior to launching Zelle, TD Bank AML personnel identified potential money laundering-related risks, including transactions involving high-risk jurisdictions. The AML team further stated existing scenarios for the predecessor service to Zelle, a much lower volume product, needed to be reviewed to determine the impact on monitoring. After Zelle was implemented, AML teams requested unique scenarios that would be appropriate for Zelle, but TD Bank ultimately did not implement ***any*** new scenarios specifically focused on this product (instead adding Zelle to certain existing scenarios).

Initially, TD Bank monitored Zelle personal transactions through scenarios used to monitor debit card transactions. In April 2020, roughly three years after launching Zelle, the Bank belatedly added unique codes to allow it to differentiate Zelle payments from other transactions executed on the Bank's debit cards. TD Bank's deployment of these unique codes allowed the AIU to include Zelle transactions within the scope of existing scenarios the Bank used to monitor personal accounts' high velocity incoming and outgoing funds transfer activity. However, these scenarios were designed to be used for wire activity and were not fit for the purpose of monitoring Zelle activity: they generated alerts only when a personal account received at least two wires or transfers with an aggregate greater than or equal to $10,000 over five business days or sent at least two cash deposits with an aggregate greater than or equal to $9,000 over five business days. Yet, Zelle has a daily transaction limit of $2,500 and a rolling 30-day limit of $10,000. TD Bank repeatedly cited these scenarios (without

[48] The following focuses on TD Bank's offering of Zelle to its retail customers.

describing the scenarios' parameters), along with even less applicable scenarios geared towards commercial customers with a $100,000 threshold, as examples of current Zelle monitoring to at least one of its regulators, even though the thresholds were not suitable to the product and TD Bank anticipated monthly alert volume for these scenarios in the single digits.

Bank personnel knew that these wire-oriented scenarios would not reasonably mitigate the risks associated with Zelle activity. One AML manager observed that because wire scenarios have high-dollar thresholds inconsistent with the types of transactions effected via Zelle and other P2P platforms, Zelle activity "[got] lost in the much bigger $ wire category." The Bank added Zelle transaction codes to five other scenarios in 2023, which all monitor for aggregate amounts ranging from $50,000 to $150,000, continuing the Bank's ineffective monitoring of Zelle activity.

AML staff also expressed specific concern with low-dollar amount Zelle transactions, especially in higher velocities. In August 2020, the Bank abandoned plans to add Zelle to certain existing terror financing scenarios because an impact analysis showed that too many alerts would be generated; instead, the Bank decided to create a new scenario unique to Zelle. In October 2020, AML personnel submitted such a request for new high velocity scenarios specific to detecting potential terrorist financing transactions effected via Zelle. However, as with other examples of extensive delays described elsewhere in this Consent Order, analysis for the potential scenario implementation was not completed until November 2021, more than a year later.

Even after eventually performing the analysis in late 2021, AML management stated that, based on "direction" they had received, the Bank would not introduce any new scenarios unless there was an "exposed risk or regulatory need" and that "unless absolutely required, new scenario development in [the transaction monitoring system] is ***regrettable spend***." TD Bank implemented the proposed scenario only in February 2023, roughly six years after Zelle's launch, two-and-a-half

years after the initial request for the scenario was submitted, and well after the Bank was aware its AML practices were facing intense scrutiny by regulators and law enforcement.

TD Bank's failure to implement scenarios addressing risks specific to Zelle, even after several AIU staff flagged potential monitoring gaps, led to TD Bank's failure to timely report suspicious activity. In May 2021, more than four years after the Bank's initial implementation of Zelle, an AIU analyst investigating transactions linked to potential human trafficking, which had been manually identified by a TD Bank employee completing an unusual transaction referral (UTR),[49] determined that many of the accounts involved in the activity transacted via P2P channels, including Zelle. However, despite the "***really big red flags***" of such activity being associated with human trafficking, no automated alerts had flagged this activity—some of which took place months before the AIU investigator became aware of it—for review. The AIU analyst provided examples to an AML senior manager of the Zelle "***activity that we are missing***" by not having a relevant scenario in the automated monitoring system.[50]

In another example, TD Bank failed to identify and timely report suspicious activity that was indicative of human trafficking and processed in part through P2P transactions. In one instance related to a purported HVAC company, the undetected suspicious activity spanned a nine-month period, from July 2023 to April 2024, and included over $3.5 million in a combination of more than 1,000 P2P transactions, as well as check deposits, withdrawals, and ACH transactions. This high volume of activity drastically conflicted with the customer due diligence documentation collected by TD Bank, which reported the maximum annual sales revenue of this customer as $500,000.

[49] Unusual Transaction Referrals (UTRs) are referrals that TD Bank's AML function receives from the Bank's business lines and other internal sources regarding unusual or potentially suspicious activity observed by employees in those business segments. Employees manually submit a UTR form, which, pursuant to Bank policy, should be triaged within 24 hours of receipt by AML.

[50] There is no evidence that the issue was escalated to executive management or the Boards.

Yet, TD Bank never questioned the ultimate source of the millions of dollars flowing through the customer's accounts over a relatively short timeframe, which was clearly disproportionate to the customer's reported annual revenue. Despite purporting to relate to operating in the HVAC industry, the suspicious transactions involving this supposed HVAC company related to interstate freight carrier services, hotels, and multiple mobile phone providers. The suspicious transactions also included purchases of hundreds of airfare tickets to high-risk jurisdictions such as Turkey, Thailand, and Colombia, and hundreds of purchases for visa immigration services in high-risk jurisdictions such as Suriname, Nicaragua, Ethiopia, and Singapore. Similarly, suspicious transactions involving this purported HVAC company also included withdrawals from ATMs across four states and multiple foreign jurisdictions, including Uzbekistan, Ecuador, and Mexico. Further, a TD Bank salesperson expressed concerns shortly after onboarding customers affiliated with the owner of the HVAC company, upon realizing one of the affiliated businesses was inappropriately operating out of a residential address. Despite the clear human trafficking "red flags,"[51] TD Bank failed to proactively identify any of this suspicious activity over nearly a year due to the known gaps in its transaction monitoring system as described above,[52] and, ultimately, filed a late SAR after prompting from law enforcement. After the Bank identified the issues with this customer, it proactively notified FinCEN of its internal investigation and subsequently filed a late SAR.

Similarly, some of the employee-related misconduct at TD Bank, identified only after one of its employees was arrested (described below), involved Zelle transactions.

---

[51] *See, e.g.*, FinCEN, FIN-2020-A008, Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity (Oct. 15, 2020).

[52] *See supra* Section II.E.2.a.

(3) Funnel Accounts

FinCEN issued an advisory in 2014 about funnel accounts,[53] and during the Relevant Time Period, TD Bank clearly understood both the risks associated with this typology and the gaps in its coverage of them, but did not implement adequate controls to manage those risks and close those gaps.

TD Bank maintains no physical presence in Latin America, yet during the Relevant Time Period, TD Bank customers conducted millions of ATM withdrawals in that region: a sample review of ATM withdrawals from five high-risk Latin American and Caribbean jurisdictions totaled more than $750 million. Moreover, within this sample, transactions in Colombia stood out as clear outliers: they accounted for nearly half of the $750 million of ATM withdrawals by dollar value and far exceeded the withdrawals in Mexico—despite the fact that Mexico's economy is roughly four times as large as Colombia's economy. Similarly, the volume of Colombian ATM withdrawals exhibited a roughly 50% annual increase each year over a four-year portion of the Relevant Time Period.

AML personnel identified customers engaged in funnel account activity in the spring of 2019. AML investigators were also aware that, with respect to funnel accounts, "***bad actors target TD*** [Bank]," including because the Bank maintained different policies than other peer financial institutions. In a one-month period in late 2020, the Bank's scenario for personal ATM activity in high-risk countries identified ***Colombia as accounting for over 90% of the triggering transactions*** in a one-month period that exceeded expected parameters.

[53] FinCEN, FIN-2014-A005, Advisory: Update on U.S. Restrictions in Mexico: Funnel Accounts and TBML (May 28, 2014) (defining a funnel account as "[a]n individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.") In 2010, FinCEN issued an advisory related to trade-based money laundering that specifically identified risks associated with ATM withdrawals made in foreign jurisdictions. FinCEN, FIN-2010-A001, Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering (Feb. 18, 2010).

Despite this awareness, TD Bank demonstrated no urgency to address the issue and failed to take sufficient measures to mitigate funnel activity risks. Moreover, even in the instances in which the Bank identified a funnel account, between October 2019 and March 2022, the Bank averaged approximately 329 days from account opening to demarket the relevant customer from the Bank.

Two years after AML personnel began raising concerns about funnel accounts, TD Bank finally developed a manual control to compensate for deficiencies in its ability to timely identify customers engaged in funnel account activity. To date, this manual control has never been subjected to appropriate testing to determine if its parameters are fit to mitigate the risks.[54]

TD Bank still has not implemented planned automated scenarios to mitigate related risks due to the extensive delays with the transaction monitoring system replacement described above. In late 2023, a third-party service provider to TD Bank notified an AML senior manager about ongoing concerns related to TD Bank's internal controls for international ATM withdrawals that were consistent with the funnel account issues described above: "the actual number of unique accounts is close to over 20,000 so it is very important to find the pattern and scheme and for TD [Bank] to tighten the controls to prevent this type of activity in the future." The third party provided the Bank with analysis identifying large and unexplained amounts of activity in Colombia, including identifying "***multiple cards that conducted withdrawals at the same ATM location, just seconds/minutes apart***." For example, the customer linked to the cards underlying these back-to-back transactions purported to be a computer repair company based in New Jersey that had no apparent commercial reason to engage in such high-risk transactions. This issue was not timely escalated to executive leadership or the Boards. In 2024, the Bank implemented additional controls to address this activity, including reduced ATM withdrawal limits in certain high-risk countries.

[54] Since its implementation, the manual control has resulted in SARs being filed and accounts being demarketed.

(4) Ineffective Monitoring of High-Risk Jurisdictions

TD Bank's pause on implementing new scenarios or changing existing scenarios also impacted its monitoring of high-risk jurisdictions. As early as 2018, the Bank's Internal Audit department found that not all jurisdictions TD Bank identified as high-risk were subject to monitoring by relevant scenarios in the Bank's transaction monitoring system. Not only did TD Bank fail to timely address this finding, but also at a subsequent meeting to discuss potential updates to the high-risk jurisdiction scenarios, AML senior management, including the BSA Officer, concluded that only proposed changes that "would have ***no impact or lower the volume of false positives*** have been approved to proceed." This meant the AIU could only ***remove*** those jurisdictions from monitoring that were no longer high-risk; the AIU was not allowed to ***add*** new jurisdictions, because doing so would increase the volume of alerts.

A subsequent review of ATM-related scenarios concluded the list of high-risk jurisdictions associated with these scenarios should be updated, but adding all high-risk jurisdictions would increase the monthly alert volume by more than 250%. Accordingly, AML personnel recommended updating the list of countries while simultaneously modifying another parameter to reduce relevant resulting alerts.

The Bank eschewed subsequent reviews of scenarios related to ATMs and wires in high-risk jurisdictions due to the ongoing transition to the new transaction monitoring system, but the Bank knew this implementation was delayed. AML personnel similarly concluded updating the list in the transaction monitoring system, while necessary to properly account for the high-risk jurisdictions in which TD Bank operated, would increase the alert volumes and add to the "sub-optimal utilization of TD [Bank] resources."

In July 2023, TD Bank discovered that a portion of international wires was coded incorrectly as domestic rather than international, and therefore not properly monitored. For example, in June

2023, "(7.31%) [of] outgoing international wires have the value "US" in the Country Code field as opposed to the actual destination country." The Bank believed this issue had "been in existence since day 1 (so could be as long as 10 years.)" and caused scenarios to miss alerts on wires sent to high-risk jurisdictions. The Bank planned to implement a solution in October 2023 to improve the quality of the country code data with the caveat that manual controls would need to continue.

b) Governance Failures

Governance and oversight failures also contributed to TD Bank's failure to implement and maintain appropriate scenarios in its transaction monitoring system. In 2018, members of the Bank's AML Risk and Monitoring team authored a "Transaction Monitoring Strategy" document which described the Bank's transaction monitoring system as "***lagging behind peer group standards***" and stated upgrades to existing tools "experience[d] frequent delays." During the drafting of the document, one AML senior manager heading this team requested that the authors revise the document to represent the current transaction monitoring system in a more "***positive***" light. The document recommended the Bank's transaction monitoring strategy should change to include "a proactive customer behavioral strategy." However, the Bank failed to meaningfully respond to these concerns, proceeding first with the delay-ridden upgrade to the system, then beginning the prolonged (and, more than five years later, yet to be completed) process of switching vendors.

As a result, TD Bank did not develop a comprehensive framework for implementing new transaction monitoring scenarios until September 2021. From 2017 to 2021, six new transaction monitoring scenarios were proposed, but none were implemented. The six new scenarios were recommended to cover gaps in the Bank's monitoring of high-risk jurisdictions and cash debits, as well as Zelle, cross-border transactions, and ATM transactions. The failure to implement these scenarios led to significant gaps in TD Bank's transaction monitoring.

These governance failures ultimately contributed to many of the Bank's failures to timely identify and report suspicious activity.

First, in 2011, AML senior management "paused" a transaction monitoring scenario targeting large cash deposits in commercial accounts; although this "pause" was framed as temporary at that time, the scenario remained dormant for at least a decade. As a result of this oversight failure, the Bank's transaction monitoring system failed to generate over 150 alerts for suspicious activity related to a scheme involving a group of TD Bank customers (Customer Group A) that purported to operate in the precious metals industry, but that bore indicia of unregistered money services businesses (MSBs).[55]

A separate money laundering scheme and unlicensed MSB operated by the Sze Network[56] also exploited a gap in the monitoring of commercial cash transactions.[57] TD Bank's failure to reinstate this scenario for business accounts caused the Bank to fail to detect suspicious activity and report it to FinCEN. Additionally, TD Bank allowed its customers to make cash deposits at its branches and purchase official bank checks from these proceeds without any entries in the corresponding customer account(s). The scenarios applicable to these large cash transactions were also defective, as they did not alert for purchases of official bank checks beyond a certain value. This created a gap in the Bank's ability to identify and report suspicious cash transactions.

Second, in 2013, TD Bank decommissioned two scenarios for funnel accounts due to "data quality" challenges. Bank personnel understood these scenarios generated SAR filings that were

[55] *See infra* Section II.E.4 and Section II.G.2.

[56] For further discussion on the Sze network, *see infra* Section II.E.3.b.

[57] *See infra* Section II.G.3. A subsequent review also found that other deficiencies in TD Bank's monitoring system also contributed to this group of illicit actors being able to use the Bank for their activities. Six scenarios did not generate alerts on these transactions due to inappropriate scenario designs, including inadequate thresholds and failure to capture different types of monetary instruments.

helpful for law enforcement, and the decommissioning was intended to be temporary while the data-related issues were addressed. However, despite subsequent requests to reinstate one of the scenarios, "no one was willing to [reinstate it]…so that scenario sits there idle going on seven or eight years now."

Finally, in 2020, TD Bank's Internal Audit department conducted a review of the Bank's AML function that resulted in a high-risk rating, in large part because there were outstanding reviews of transaction monitoring scenarios, as well as recommended changes to scenarios that were overdue due to defects stemming from the transaction monitoring system upgrade. In response, an AML senior manager acknowledged the need to add new scenarios to the transaction monitoring system but noted budget constraints. The AML senior manager described this failure of scenario development as a "***glaring risk***."

c) Testing Issues

TD Bank conducted several scenario "tunings" from 2017 to 2021. In theory, scenario tuning should test the performance of scenarios by looking at both false positives and missed suspicious activity. However, early in the Relevant Time Period, TD Bank's scenario tunings focused on SAR conversion rates and changing scenario thresholds to minimize false positives, although the Bank looked at limited opportunities to capture additional intended risk. A 2015 Model Validation found the approaches to scenario tuning "were not statistically adequate" and recommended a new tuning methodology. Although the Bank subsequently accepted and implemented the new tuning methodology, its approach to scenario testing continued to be subject to other issues.

TD Bank failed to reasonably assess whether the scenarios it maintained adequately mitigated the money laundering risks that the Bank faced. A 2017 Model Validation found that even though an AML group performed an assessment to evaluate gaps, the typologies that the AML group used were too broad to effectively evaluate the scenarios' mitigation of the Bank's risks. The report

recommended the AML function develop a "more comprehensive adjustment that pays attention not only to avoiding false positives but also to capturing true positives." Although TD Bank eventually implemented a process to review scenarios in order to address these concerns, this occurred nearly a decade after it initially implemented its transaction monitoring system, and many of the reviews were still outstanding in 2020, several years after the process was first developed.

According to a 2020 internal audit, ***half of the transaction monitoring scenarios' mandatory reviews remained outstanding for three years***, with no overall target date for completion. Moreover, the 2020 audit also found that, for the scenarios with completed reviews that included recommended changes, implementation work was not performed in a timely manner. Finally, until late 2021, the Bank did not maintain any procedures or formal documents outlining processes for either the promotion of new scenarios in the transaction monitoring system or in a manual environment to capture any triggers or market-driven factors, such as the impact of COVID-19.

3. Training Gaps and Deficiencies

Until near the end of the Relevant Time Period, TD Bank's AML management failed to properly ensure the requisite employees received appropriate training. The issues included: (i) a lack of tailoring to appropriate personnel regarding relevant risks and typologies; (ii) insufficient direction on evaluating and responding to UTRs, as frontline personnel were encouraged to stop reporting potentially suspicious activity; and (iii) improper training related to filing of CTRs, which contributed to employees' provision to law enforcement of misleading information.

a) Failure to Tailor Training to Appropriate Personnel and Relevant Risks

Despite awareness that it faced elevated risks of specific money laundering typologies in certain regions, the Bank did not tailor its training program for both AML compliance personnel investigators and "frontline" retail branch personnel. For example, as discussed above, in 2019, the

Bank identified an increasing trend of apparent funnel account activity, including multiple debit cards linked to the same account being used to withdraw large amounts of cash via ATMs in high-risk jurisdictions. Even after developing potential red flags and a methodology to identify the accounts, AML personnel did not provide updated training to retail employees or visit branches identified as onboarding the high-risk customers. Instead, in the four years since AML personnel first began tracking this risk, the Bank conducted only one training, in 2020, to a subset of its branches that contained a single sentence regarding the risks of ATM withdrawals. In 2023, the Bank conducted additional trainings that addressed specific issues, including funnel accounts.

b) Improper Training Related to Unusual Transaction Reports (UTRs)

The Bank's manual processes around UTRs included training-related deficiencies, particularly with respect to (i) specialized red flags for higher-risk activities, and (ii) more fundamental concepts as to how and where to file UTRs. The AIU analysts who reviewed UTRs often missed money laundering typologies or provided incorrect guidance to other Bank employees.

In one example, personnel working at a retail branch submitted a UTR raising concerns about potential collusion of two individuals—later determined to be part of the Sze network—who deposited large amounts of cash at different branches and ATMs. The individuals mentioned in the UTR were ultimately indicted for their involvement in a larger money laundering ring that effected a significant portion of its transactions through TD Bank: in February 2022, Sze pled guilty[58] for his role in coordinating a vast money laundering conspiracy, operating an unlicensed MSB, and bribing bank employees. From 2016 through 2021, the Sze Network laundered an estimated $650 million in

[58] DOJ, Queens Man Admits Orchestrating $653 Million Money Laundering Conspiracy, Operating Unlicensed Money Transmitting Business, and Bribing Bank Employees (Feb. 22, 2022).

cash, consisting of narcotics and other illicit proceeds, utilizing TD Bank and other institutions. The Sze network conducted more than $400 million in transactions through the Bank.

Despite collusion by Sze's associate—as mentioned in the UTR—as well as the AIU investigators' identification of a recent SAR for the same individual, TD Bank investigators failed to use salient information from the UTRs as a basis for preparing SARs. For example, a May 2020 UTR clearly identified two members of the network "working together" to engage in cash activity at multiple branches and ATMs. However, the corresponding SAR failed to clearly explain such information, including identifying both the relevant persons named in the UTR as subjects of the SAR. This deprived law enforcement of information that would have allowed for faster identification and prosecution of Sze and his co-conspirators.

Branch personnel continued to have concerns about these individuals and corresponding customer accounts, and as required by Bank policy, they submitted additional UTRs. However, an AIU manager informed branch personnel they no longer needed to send additional UTRs for unusual activity about these individuals and corresponding customer accounts that occurred for the next six months because they were already under investigation. Coupled with other instances in which Branch personnel were told not to file additional UTRs on the same activity, even when the unusual activity continued, certain branch employees assumed the ongoing activity was deemed appropriate by AML management.

c) Improper Training Related to Filing of CTRs

TD Bank's training deficiencies led to employees filing numerous CTRs without recording all of the individuals present for transactions and accepting photos of identification on phones for persons not physically present at the bank branch. For example, the Sze Network routinely accepted illicit proceeds and then deposited the cash into approximately 100 TD Bank branches in New York, New Jersey, Pennsylvania, and elsewhere, utilizing bank accounts in the names of shell companies

and conspirators. The Sze Network then further obfuscated the source of the illegal cash by purchasing official bank checks, writing personal and business checks, and making international and domestic wires to jurisdictions like Hong Kong, which can pose a higher risk for a North American-focused bank like TD Bank. The Bank did not properly record Sze on over 100 CTRs, and instead Bank branch personnel reported only the accountholder, who on many occasions was not present and, in at least one instance, accepted a photo of the accountholder's identification that Sze showed a Bank employee on Sze's phone.

The branch employees clearly recognized Sze, as he routinely provided gift cards to employees of TD Bank when he visited branches. In 2020 and 2021, Sze provided at least $57,000 in gift cards to financial institution employees in connection with financial transactions. However, some of the branch employees later indicated they believed they were not required to name the individual(s) transacting where the customer was also present for the transaction, despite FinCEN's clear instructions for filing CTRs.[59]

4. Customer Due Diligence Systemic Deficiencies

TD Bank failed to implement and maintain appropriate risk-based customer due diligence (CDD) procedures, which significantly impeded the Bank's ability to understand their customer base and associated risks.[60] The Bank failed to sufficiently collect and review information required to develop an adequate customer risk profile and identify high-risk accounts. Further, the Bank's

[59] FinCEN, FinCEN Currency Transaction Report (FinCEN CTR) Electronic Filing Requirements, version 1.2 (July 2013), p. 48 (providing that "[a]ll individuals…conducting reportable transactions for themselves or for another person, must be identified by means of an official document.") (emphasis added); see also 31 C.F.R. § 1010.312 (" … a financial institution shall 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.").

[60] 31 C.F.R. § 1020.210(a)(2)(v).

failures to remediate numerous and longstanding issues with its customer risk rating system led to significant deficiencies in the ongoing monitoring of high-risk customers.

a) Failures to Sufficiently Collect and Review Information to Develop an Adequate Customer Risk Profile

The Bank's CDD policies and procedures were deficient, as information obtained about customers at account opening and the Bank's analysis of such information was inadequate to properly assess the customers' risk and support the Bank's effective suspicious activity monitoring. For example, in February 2021, when the Bank onboarded accounts for Customer Group A, the New York companies purporting to operate in the precious metals industry, the Bank collected information about the customers' expected activity as well as financial information about the companies' operations. Almost immediately after account opening, the customers began bringing large volumes of cash deposits to TD Bank branches, and branch personnel soon expressed concern about this activity.[61] However, the Bank failed to properly consider Customer Group A's high volume of cash deposits as part of the Bank's AML risk profile for the relevant accounts. Instead, the Bank focused primarily on its operational (but not AML-related) risks by enrolling these customers in armored car services. In doing so, the TD Bank sales team acknowledged that in the onboarding of these customers, "***the cash is what is making this [relationship] so lucrative***," but remained nervous about the large volume of cash, since the AIU sought documentation from the sales team to legitimize the cash deposits. The Bank took other steps to accommodate these customers, including waiving fees, as gestures of good faith. Over time, these customers continued to increase their cash activity through the Bank. However, the Bank collected the customers' financial statements and tax returns only after Customer

[61] A retail branch manager wrote, "[w]ork with [the Bank's Treasury Management] to get this volume out of the [branch]." TD Bank eventually learned that another bank had maintained accounts for Customer Group A, but that the other bank had closed the accounts after being open for less than a month; this closure was contemporaneous with Customer Group A's initial activity through TD Bank.

Group A applied for a lending product; this financial information that Customer Group A eventually provided to the Bank contained numerous inconsistencies and red flags that the activity was not supported by legitimate operations. TD Bank personnel continued to allow these customers to conduct large volumes of transactions through the Bank for roughly a year, until after receiving additional inquiries from law enforcement about these customers.[62]

The Bank also failed to ensure sufficient information regarding the nature of customers' businesses was obtained at account opening and maintained during the life of the relationship. For example, after receiving an inquiry from law enforcement in 2022 related to alleged drug trafficking, the Bank initiated an investigation into a Florida-based customer purportedly operating in the computer manufacturing industry. Upon investigation, the prior due diligence failures became immediately apparent, as the Bank determined from the product reviews of electronics listed on the customer's public website that the company was purportedly selling prescription drugs. Further, the Bank's investigation identified red flags pertaining to the address on file for the customer, namely that it was a residential address shared by several other TD Bank customers, including entities that were also purportedly operating in the electronics and computer industry. The customer remitted and received millions of dollars with the accounts of other TD Bank customers at its address, and also received wires, including from high-risk jurisdictions such as Paraguay, the Dominican Republic, and Panama. In sum, TD Bank failed to detect and act on red flags, allowing a continuation of customer relationships that posed heightened and unmitigated risks until after the Bank received an inquiry from law enforcement.

[62] For a discussion of the late filed SARs, *see infra* Section II.G.

b) Failures to Remediate Numerous and Longstanding Issues with the System Used to Identify High-Risk Customers

TD Bank's process for identifying and assessing high-risk customers was insufficient and improperly administered due to TD Bank's inadequate staffing and failure to maintain the necessary software. The failure to maintain such software led to extensive system-related deficiencies, similar to those associated with the Bank's transaction monitoring system (as described above). These issues spanned both the Bank's primary risk rating system for its customers, as well as related data feeds and processes.

Throughout the Relevant Time Period, AML senior management frequently reported issues with the Bank's primary customer risk rating system. In January 2019, the Bank identified at least 65 unresolved issues involving this system that spanned from 2016 to 2019. One such outstanding issue pertained to risk scores for certain customers that were displaying a string of arbitrary numbers, instead of the proper date, time, and score. Around the same time, an AML senior manager acknowledged a subset of customers were inadvertently omitted from scoring, which resulted in the identification of more than 500 U.S.-based high-risk customers that had not been previously identified as posing a high risk by the Bank's AML group. However, the Bank took no steps to scrutinize this population of customers or the transactions they had effected through the Bank while they were not classified as high-risk customers.

These issues also extended to other systems and processes that were integral to effective customer risk rating. In 2019, the BSA Officer and AML senior management were informed that certain updated risk-related information was not linked to the related customer records because updates made to customer data while a computer memory issue persisted were not factored into a customer's risk rating score. This resulted in the Bank failing to integrate accurate information necessary for proper risk monitoring.

In June 2019, the BSA Officer informed a Bank risk management committee that projects intended to strengthen the Bank's customer risk-rating system and related processes were delayed due to technology and funding issues. The BSA Officer assured the committee these projects would get back on track by August 2019.

However, in September 2019, the risk-rating projects remained in "red" status, with revised planning efforts then just getting underway. At the same time, AML personnel reported to another risk management committee of senior executives, including the BSA Officer, that a backlog of ***1.6 million customers*** had been identified that were never scored for risk rating. The members of this executive committee, including the BSA Officer, debated the approach the Bank should take for this population of customers. This included consideration of the results of a small sample analysis which indicated that the number of high-risk customers within this unscored, larger population may have exceeded 200,000 customers. The committee members ultimately recommended against any remedial work specific to this large population of unscored customers, in part because it would compete with ongoing risk-related projects and resources. Instead, the members of the committee discussed the importance of Bank personnel "***align[ing] on messaging to regulators***" regarding customer risk-rating processes.

The same committee later identified another risk rating issue that pertained to account linkages, in which certain customers were either not scored or were incorrectly scored, due to customer accounts improperly linking to unique identifiers assigned by the Bank. This issue resulted in ***approximately 5.2 million unscored accounts related to more than 2.5 million unique customers***. Despite the fact the issue was first identified five months earlier, the report to the committee indicated personnel were still working to identify the root cause and categorized the issue as "complicated" and requiring "extended analysis," with no immediate resolution proposed.

In November 2019, AML senior management acknowledged all ongoing customer risk rating projects would be delayed until mid-2020, with a final resolution date of February 2021. However, in April 2020, the committee identified additional projects required to remediate the customer risk rating processes, many of which had been deferred due to resource constraints.

In 2023, the Bank implemented a new customer risk scoring methodology as part of its migration to another risk rating system. However, this required the Bank to rescore all its customers and complete a remediation of data inputs. This data remediation for the Bank's highest risk customers is underway but is not yet completed.

c) Significant Deficiencies in the Ongoing Monitoring of High-Risk Customers

TD Bank's AML function maintains a High-Risk Customer (HRC) Group based upon risk ratings determined by the issue-laden risk-rating processes described above. HRCs are classified as either Tier I or Tier II[63] based upon their potential money laundering and terrorist financing risk. The Bank's HRC procedures mandate the highest risk customers, those belonging to Tier I, are subjected to the most frequent application of review and the highest degree of enhanced due diligence (EDD). However, in practice, the Bank failed to implement controls sufficient to address risks associated with Tier I and Tier II HRCs.

For example, the Bank's highest risk customers in Tier I were not subject to comprehensive transactional reviews to assess whether Tier I customers' use of the Bank's products and services was consistent with TD Bank's risk profile for that customer. TD Bank required only a 90-day review

[63] The Bank's Tier I HRCs are defined as customers with business activities that inherently pose a significant money laundering risk. The Bank's High Risk Review Procedures classify Tier I HRCs as those that include customers such as issuers of bearer shares, precious metals dealers, financial institutions designated under Section 311 of the USA PATRIOT Act, foreign casinos, internet gambling organizations, virtual currency exchangers, weapons brokers, and unregistered charitable organizations. The Bank's Tier II HRCs are defined as customers identified as high-risk through the Bank's risk rating process and not included in Tier I.

window of transactional activity. These limited reviews of Tier I HRCs and their transactional data resulted in the Bank failing to monitor customers in a risk-based manner and exposed the Bank to significant risks.

For example, in July 2019, the Bank onboarded accounts for a New York-based religious institution despite its leader's ties to terrorist organizations and involvement as an unindicted co-conspirator in the 1993 World Trade Center bombings. Despite this publicly available negative news, TD Bank failed to perform adequate due diligence at account opening and failed to understand its customers' terrorism-related associations.[64] As a result, the Bank failed to categorize this customer relationship as high-risk, consequently failing to perform EDD reviews and properly monitor its transactions.[65] As a result of a recently implemented scenario designed to look at changes in customer behavior—a foundational red flag used to identify and report suspicious customer activity[66]—TD Bank ultimately filed a SAR on this customer in April 2024, but acknowledged the suspicious activity indicative of terrorist financing began ***four years prior***, shortly after the customer was onboarded by the Bank. From approximately April 2020 to March 2024, TD Bank processed over $3 million in suspicious transactions for this customer, which included deposits from crowdfunding platforms,[67] charitable institutions, donations from individuals and businesses, unknown remitters utilizing a West

[64] The only negative news screening documented for this customer relationship was completed on May 29, 2024.

[65] TD Bank inappropriately risk-rated this customer relationship as "medium" risk, thereby resulting in a failure to perform EDD reviews.

[66] *See, e.g.*, FinCEN, FIN-2011-A016, Advisory: Account Takeover Activity (Dec. 19, 2011) (describing deviations from "a customer's normal activity" that could be red flags of cybercrime); FinCEN, FIN-2022-A002, FinCEN Advisory Elder Financial Exploitation (Jun. 15, 2022) (describing red flags of elder financial exploitation, including "unexplainable or unusual account activity," "[u]ncharacteristic, sudden, abnormally frequent, or significant withdrawals of cash or transfers of assets," and "[u]ncharacteristic attempts to wire large sums of money"); FinCEN, Money Laundering Prevention: A Money Services Business Guide, ("Be alert for changes in activity," such as "[m]ajor changes in customer behavior" and "[s]udden and inconsistent changes in money transfer send or receive transactions").

[67] According to the 2024 National Terrorist Financing Risk Assessment published by the U.S. Department of the Treasury, crowdfunding platforms are an emerging trend in terrorist financing. U.S. Department of the Treasury, 2024 National Terrorist Financing Risk Assessment (Feb. 2024).

Africa-based MSB, and bulk cash and check deposits totaling approximately $1 million from possible shell companies. This volume of activity significantly varied from the customer's reported expected activity, in which the customer claimed its anticipated cash deposits and wire transfer activity would not exceed $50,000 on a monthly basis. TD Bank's delays in identifying and reporting this customer's activities illustrate weaknesses in the Bank's CDD process, including failing to timely investigate a significant discrepancy between expected and actual activity. As a result, the Bank failed to detect and report these indicators of terrorist financing sooner, depriving law enforcement of an opportunity to intervene earlier. After the Bank identified the issues with this customer, it proactively notified FinCEN of its internal investigation and subsequently filed a late SAR.

TD Bank's Tier II HRCs were subjected to even less scrutiny, requiring a periodic review only every 24 months, and, more significantly, provided no requirement for ***any*** transactional review as part of the periodic reviews. This approach to monitoring Tier II HRCs failed to properly mitigate the Bank's risks.

The EDD and periodic reviews performed for the Bank's HRCs were of insufficient depth and impeded the Bank's ability to understand risks within customer relationships. The Bank failed to apply the appropriate operational rigor required to successfully address the risks associated with its highest risk customer base. For example, in or about 2010, the Bank onboarded a Pennsylvania-based company that purported to operate as a travel agency and opened hundreds of related accounts for this high-risk customer, even though the Bank did not have a clear understanding of the customer's expected activity and the parties with whom it expected to transact. This customer's accounts remained open throughout the Relevant Time Period and routinely engaged in excessive cash activity—including withdrawals at ATMs in foreign jurisdictions, the frequency and volume of which were inconsistent with this type of business—with the Bank filing nearly 2,000 CTRs for cash activity

with an aggregate value of over $85 million for this customer. The Bank did not reassess this large volume of transactional activity as part of the customer's risk profile, and failed to file SARs on this cash activity that exhibited clear indicia of suspicion. At the same time, the business line focused on the customer's revenue to the Bank by tracking variances in this customer's account activity as part of the Bank's monthly revenue reporting.

TD Bank further failed to deploy automated transaction monitoring in a differentiated manner based on the risks of its customers. Such tailoring, which the Bank referred to as "segmentation," enables a financial institution to apply controls to customer activity on a risk basis and allows for effective monitoring of suspicious activity. As early as 2017, the BSA Officer and AML senior management identified customer segmentation as a key initiative for the Bank, as it would allow for a risk-based approach to reviewing customer transactions. Throughout the Relevant Time Period, AML personnel attempted to plan this proposed customer segmentation effort, but were continuously hampered by the Bank's transaction monitoring system, including the delayed software upgrade described above. The vendor for this system also issued a report to the Bank recommending that, before attempting to implement segmentation, the Bank first address alert aggregation methodology and ensure all alerts were being closed with a true understanding of worthiness. In making this recommendation, the vendor noted that the Bank's decision to use an older version of a transaction monitoring system severely limited the Bank's ability to calibrate AML scenarios.

Failure to establish an effective CDD program and critical, ongoing issues with the Bank's customer risk rating processes allowed millions of high-risk customers to remain unscored during the Relevant Time period, which significantly impeded the Bank's ability to monitor its customer base and properly address associated risks.

5. Independent Testing

TD Bank's independent testing function was ineffective and, as with the other pillars of TD Bank's AML program, the approach to testing was insufficiently grounded in the actual illicit finance risks that the Bank faced.

First, TD Bank's scope of testing was insufficient relative to the Bank's high-risk customers, products, and services. For example, during the Relevant Time Period, TD Bank's audit function performed multiple tests of the Bank's controls related to physical cash, but such testing included only a limited review of AML controls. As a result, the Bank failed to detect the cash-related control gaps described above. Furthermore, the Bank also failed to appropriately test coverage assessments resulting in trillions of dollars going unmonitored for the entire Relevant Time Period.

The Bank's methodology to assess risk across its entire AML program, via its annual assessments, was inadequate and overlooked key risk and control factors that materially impacted the analyses of the Bank's risk profile. The assessments lacked depth and specificity, which prevented AML management from accurately assessing the BSA/AML risks associated with TD Bank. Inaccurate risk assessments, which included inconsistent risk ratings of certain bank products, demonstrate the Bank lacked an understanding of the illicit financial activity risks within the products and services it offered.

Second, the Bank failed to properly prioritize AML-related risks in planning processes related to testing. AML risks were not independently rated for assessment, and the Bank repeatedly failed to assess such risks as part of its testing processes.[68] Similarly, in the testing of the Bank's AML risk assessment process, internal audits simply determined whether controls existed and not whether they were, in fact, being appropriately used.

[68] *See supra* Section II.2.a.

Finally, reports of independent testing to the Bank's Audit Committee generally failed to highlight BSA-related findings, which prevented the Audit Committee from properly overseeing the remediation of BSA-related deficiencies.

F. Violations of the Requirement to File Currency Transaction Reports

CTR reporting requirements play a significant role in FinCEN's core mission to safeguard the financial system from illicit use through the collection, analysis, and dissemination of financial intelligence. FinCEN and law enforcement depend on the accurate and timely filing of CTRs by financial institutions to develop an understanding of the movement of such funds, which may be associated with several cash-based money laundering typologies. As explained further below, TD Bank's violations of CTR requirements involved two main deficiencies: (i) late filings caused by a combination of longstanding and known technological issues; and (ii) willfully filing more than 1,000 inaccurate CTRs, some of which not only failed to meet regulatory reporting requirements but also misled law enforcement.

FinCEN's investigation identified more than 4,000 late-filed CTRs covering more than $150 million in cash transactions filed weeks after the required deadline.[69] Throughout the Relevant Time Period, the Bank identified longstanding challenges with a vendor used to support its CTR filing process, with an October 2018 report acknowledging recent improvements led to "somewhat of a normal state" by bringing down the monthly numbers of late filings from "***300+ and in some [months] the 1,000 range***." Even later in the Relevant Time Period, the Bank found that nearly half of its CTR batch filings were not successfully sent to FinCEN. AML senior management identified the causes of certain of these late-filed CTRs, including the inability to "track all cash transactions to reconcile what should have been filed compared to what was filed" in CTRs, resulting in outstanding

[69] *See supra* Section II.E.1.a; 31 C.F.R. § 1010.306(a)(1).

CTRs roughly six months after the filing deadline. For example, the Bank's poor controls and lack of oversight allowed an issue related to late batch-filings of CTRs to remain unidentified for months, resulting in hundreds of late CTRs.

During the Relevant Time Period, TD Bank also filed more than 1,000 CTRs with incomplete and erroneous information, and in many instances, failed to collect any form of identification information (*e.g.*, social security number) for parties conducting transactions. The Bank has been aware of this issue since at least 2019, when the Bank learned that its CTR application failed to verify whether an identifier (*e.g.,* social security number) was collected within a CTR. The Bank failed to promptly address this issue, and as of 2021, the defect remained unresolved. The Bank considered it a low priority, postponing any effort to implement a resolution.

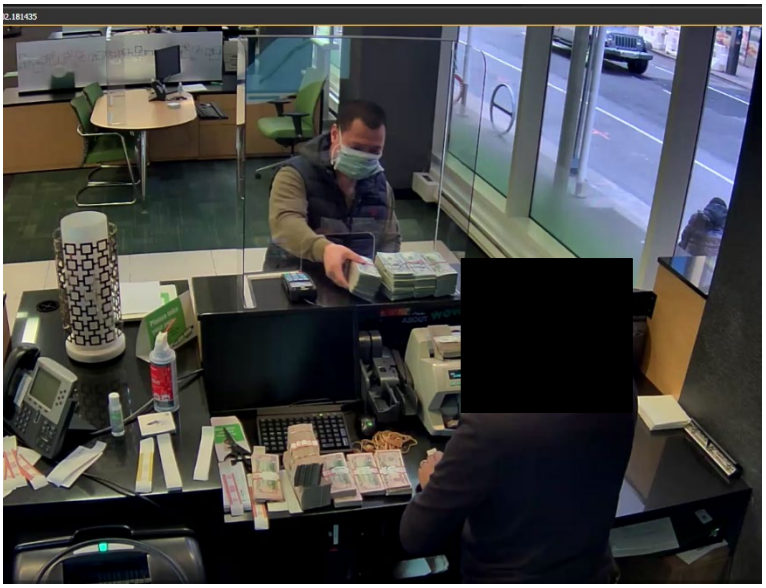
TD Bank's filing of numerous inaccurate CTRs also hampered law enforcement investigations. Specifically, the Bank failed to report the individual conducting the transaction or collect accurate identification information about the customer, as required by CTR requirements, and thus failed to accurately report more than 500 CTRs covering transactions totaling more than $400 million tied to Sze.[70] By misidentifying the conductors of these transactions, TD Bank impeded law enforcement's and FinCEN's ability to identify and track potentially unlawful behavior. Further, the incorrect CTRs misled law enforcement and caused the investigators to incorrectly expend time and resources focused on the wrong subject.

Bank personnel processing these transactions knew Sze's identity, but repeatedly accepted identification belonging to other individuals, including in at least one instance mentioned previously, wherein Sze presented to branch personnel a photo of a license on his phone. This led TD Bank to intentionally report incorrect driver's license numbers and misidentify the true individuals conducting

[70] *See supra* Section II.E.3.b.

the transactions in the CTRs. Even in the limited instances when the Bank filed CTRs listing Sze, it sometimes misattributed identification (*e.g.*, driver's license number) of his co-conspirators—the TD Bank account holders and others whose information Branch staff listed in the CTR by TD Bank.

Example of CTR violation:



The image above reflects Sze at the counter, but he is not mentioned in the CTR, which lists 29 locations and involved over $3 million in cash deposits.

G. Violations of the Requirement to Report Suspicious Transactions

TD Bank failed to adequately monitor, detect, and timely report suspicious activity. As described above, TD Bank willfully failed to implement and maintain its AML program, which included failing to maintain an adequate transaction monitoring system and staff to review alerts and investigate cases for possible reporting to FinCEN. TD Bank underreported amounts in multiple money laundering networks and missed the involvement of employees who facilitated suspicious transactions. FinCEN identified thousands of suspicious transactions totaling approximately one and a half billion dollars for which TD Bank failed to timely and accurately file a SAR. The following

six examples illustrate the Bank's failures to identify and report suspicious transactions and the resulting harm that this caused the U.S. financial system.

1. Late Filed SARs

As explained above, TD Bank's persistent underinvestment and lack of resourcing caused substantial and persistent backlogs to develop in its investigations of potentially suspicious activity. AML senior management was well aware of the duration and extent of these backlogs yet did not make sufficient and timely investments to reasonably resolve them. Instead of treating the issue with the urgency required, the Bank followed plans to "***gradually reduce***" such backlogs. In the instances in which the Bank spent limited additional funding, it did so only after business cases could be made by AML personnel, such as paying for employees' overtime to work through the mounting backlogs. At times, alerted activity went unreviewed for months. As a result, the Bank's lengthy backlogs of investigations delayed the timely notification of suspicious activity to law enforcement.

During the periods of these backlogs, TD Bank willfully failed to timely file over 6,000 SARs. The aggregate value of this late-reported suspicious activity exceeded $500 million.

2. Customer Group A

Of the missed and improperly reported suspicious transactions identified by FinCEN, over 1,000 were transactions processed for Customer Group A, primarily from 2021 to 2022, with an aggregate value of roughly $200 million.[71] Most of this activity consisted of unreasonable cash activity that exceeded, within a short timeframe after account opening, both the expected cash activity on the account as well as what could reasonably be supported by the financial statements that Customer Group A provided to TD Bank as part its CDD processes. Moreover, the pattern of activity exhibited other clear indicia of suspicion, with over 99% of the cash deposited transferred out to other

[71] Customer Group A is a network of precious metals companies in New York. *See supra* Sections II.E.2.b and II.E.4.a.

banks soon after the cash was deposited at TD Bank, including to overseas accounts. At times, some of these accounts moved millions of dollars in cash in a single day, and branch employees submitted UTRs for "excessive" in-branch cash activity. However, the Bank did not file any SARs on this activity until April 2022, more than a year after the activity began and after receiving multiple subpoenas.

In addition to the Bank's CDD failures, other control gaps contributed to TD Bank's failure to timely identify and report Customer Group A's suspicious transactions. For example, the Bank's transaction monitoring system "paused" a scenario to monitor large cash deposits of business accounts, which resulted in over 150 alerts not generating.[72] Moreover, deficiencies in the Bank's investigative processes contributed to the Bank's failure to report Customer Group A's suspicious transactions: Bank personnel investigating Customer Group A's transactions that generated alerts closed them if the counterparty contained words such as "jewels" on the assumption that such the activity was not suspicious because the transaction was between parties in the same industry, even in instances where the activity exhibited other red flags (such as excessive cash, as noted above) or the counterparty was subject to adverse media.

3. Sze Network

Of the missed and improperly reported suspicious transactions identified by FinCEN, over 4,000 of these were transactions processed for Sze's Network, primarily from 2017 to 2021, with an aggregate value of more than $200 million. Sze laundered these funds primarily through cash, and TD Bank did not timely file SARs despite numerous red flags. Surveillance footage indicated that,

[72] *See supra* Section II.E.2.b.

for years, Sze conducted transactions at TD Bank on behalf of other customers' accounts, even after TD Bank had previously identified Sze as having been involved in suspicious activity.[73] TD Bank's failure to timely limit or restrict Sze's activity resulted from the Bank failing to reasonably respond to clear red flags. First, despite the customers effecting this activity purporting to operate in the clothing or textile industries (which are not known to be cash-intensive businesses), they were some of the most active Bank customers processing cash transactions. Second, much of this cash activity took place, and even increased, during the COVID-19 pandemic when most cash-intensive businesses were conducting far lower levels of transactions. Third, branch personnel filed repeated UTRs with the Bank's AML group (until AML personnel instructed Branch employees to stop filing such UTRs for extended periods of time up to six months)[74] without taking action to mitigate the recurring suspicious activity. Finally, as described above in the discussion of the Bank's CTR failures, Sze's transacting in cash through accounts that were not his own should have also presented a significant red flag to the Bank.

Further, TD Bank did not file SARs on over $125 million in cash used to purchase official bank checks by Sze and his network due to a gap in its monitoring controls and failed to identify wires to and from foreign jurisdictions as well as large checks for round dollar amounts as suspicious. In the SARs TD Bank filed involving the relevant accounts,[75] the Bank only occasionally and inconsistently referenced Sze in the narrative, even though he conducted the majority of the underlying transactions at the retail branches. Finally, TD Bank listed Sze as a subject in only six

[73] *See supra* Section II.E.3.b.

[74] AML investigators also provided this advice to cease filing UTRs for extended periods of time for matters unrelated to the Sze network.

[75] Ultimately, TD Bank filed SARs on over $300 million in transactions by Sze and his network (representing over 70% of all transactions conducted by the Sze network), though many of these SARs—covering a significant portion of the activity—were not timely.

SARs that captured less than 10% of the illicit activity that Sze conducted through TD Bank. Even after being directly told by law enforcement that Sze conducted the transactions, the Bank chose not to correct any of the relevant SARs for almost two years.

4. Individual A

Of the missed and improperly reported suspicious transactions identified by FinCEN, Individual A, a TD Bank retail branch employee, conducted several transactions totaling more than $100,000. Due to backlogs, the Bank failed to timely file on the suspicious activity in Individual A's personal account, filing a SAR over a year after two wires totaling over $35,000 that had alerted for funds rapidly moving through Individual A's account.

More egregiously, beginning in early 2021, Individual A exploited their position to facilitate money laundering activities in exchange for bribes. During their tenure at the Bank, Individual A opened over 2,000 accounts whose account holders conducted ***more than 600,000 transactions aggregating to over $200 million, many of which were shell companies with nominee owners***.[76] In return for their role in facilitating the funnel accounts, Individual A received thousands of dollars in bribe payments. Certain of the accounts opened by Individual A were then used to launder narcotics proceeds, including to Colombia. Individual A assisted the money laundering efforts by giving those who provided bribes online access to the accounts, along with dozens of debit cards for the accounts that were used to withdraw cash from ATMs in Colombia. Individual A received bribes for opening these accounts and often violated a Bank requirement that branch personnel only open accounts when customers are physically present in the branch. Individual A also attempted to lift account freezes and unblock Zelle restrictions placed on certain of these accounts.

[76] A subset of these accounts opened by Individual A, including accounts opened for apparent shell companies that were issued multiple debit cards, conducted nearly $60 million of transactions (accounting for roughly 25% of the total transactional activity associated with all accounts opened by Individual A), more than $25 million of which were ATM withdrawals in Colombia

For many of the accounts, the Bank failed to timely file accurate SARs and considerably delayed closing the accounts, which allowed millions of dollars' worth of suspicious activity to continue to flow unobstructed through the Bank. For example, five of the accounts Individual A opened cumulatively conducted over $20 million worth of transactions before the Bank ultimately closed their accounts. These five accounts were established for companies[77] incorporated in the United States and controlled by Colombian nationals. For an average of eight months,[78] the five accounts conducted transactions that exhibited clear indicia of funnel account activity,[79] including the receipt of approximately $12 million in wire transfers[80] followed by $12 million in cash withdrawals at ATMs in Colombia. TD Bank failed to timely report this suspicious funnel account activity and took an average of five months to file SARs on the five accounts. Further, the SARs filed were consistently incomplete and of limited value to law enforcement, as they failed to reflect Individual A's readily apparent involvement in the activity. Despite the high volume of suspicious activity, and the red flags associated with the rapid movement of funds involving a high-risk jurisdiction such as Colombia, it took TD Bank an average of eight months to ultimately close the five fraudulent shell company accounts.

[77] The companies' purported industries included electronic and precision equipment, computer programming, janitorial services, long-distance trucking, and security system services.

[78] TD Bank closed the five accounts an average of eight months after the accounts were opened. The transactions described above were conducted throughout this period of time.

[79] Funnel account activity often involves a customer structuring currency deposits into an account in one geographic area, with the funds subsequently withdrawn in a different geographic region with little turn-around time. The rapid flow of funds may also span a large geographic area between the deposits and withdrawals, including instances where the deposit location is thousands of miles away from the withdrawal location. FinCEN, FIN-2011-A009, Information on Narcotics and Bulk Currency Corridors (Apr. 21, 2011).

[80] Cryptocurrency-related companies remitted approximately $1.7 million of the incoming wire transfers. TD Bank could not fully identify the other wire remitters.

5. Customer Group B

Of the missed and improperly reported suspicious transactions identified by FinCEN, over 300 were transactions processed for Customer Group B, primarily from 2018 to 2023, with an aggregate value of roughly $1 million. These transactions, including nearly $15,000 through Zelle, were linked to human trafficking at massage parlors and money laundering. Since the majority of incoming funds to Customer Group B's accounts were in the form of cash and other unattributable sources, TD Bank lacked an understanding of the origin of funds going into Customer Group B's accounts. TD Bank did not report this suspicious activity until nearly five years after it began. As previously described above, TD Bank did not tailor transaction monitoring scenarios to address the risks of Zelle. TD Bank's failure to identify the Zelle suspicious activity stemmed directly from this failure. By 2021, the Bank was aware that Zelle transactions at the Bank may have links to human trafficking. The Bank failed to update its transaction monitoring scenarios, ignoring internal recommendations to implement such scenarios. As a result, the Bank failed to effectively monitor or report suspicious Zelle activity linked to human trafficking throughout the Relevant Time Period.

6. Individual B

Of the missed and improperly reported suspicious transactions identified by FinCEN, several were transactions processed for Individual B, primarily from 2021 to 2023, with an aggregate value of nearly $100,000. Individual B worked at a TD Bank branch in Florida from 2015 to February 2023 and held at least two personal accounts at TD Bank. From November 2021 through February 2023, Individual B engaged in suspicious cash activity and wire transfers for the benefit of their relatives in Cuba. Individual B claimed to use the cash to facilitate payments to international buyers on behalf of their family in Cuba. However, there were no receipts of sale to confirm their statements. TD Bank's untimely internal investigation eventually found Individual B abused their position as a TD

Bank employee and involuntarily terminated Individual B in February 2023, roughly two years after the relevant transactions began. In at least one instance, Individual B used a private room at a TD Bank location to accept a cash payment from an unidentified individual. In a separate instance, Individual B used a photo of themselves wearing a TD Bank name tag as proof of identification to alleged buyers to provide assurance.

On another occasion, a Cuban national made a cash deposit into Individual B's personal TD Bank account, using a deposit slip Individual B falsely pre-populated. TD Bank failed to file a CTR for not only the cash deposit (which exceeded the reporting threshold), but also the two offsetting cash withdrawals that occurred less than a month later. All three transactions were processed by a former TD Bank branch manager who was suspected of colluding with Individual B and intentionally circumventing reporting requirements and AML escalation.

TD Bank's investigation did not reference potential Cuba sanctions issues, and personnel involved in this investigation failed to escalate such concerns. Moreover, the Bank did not file a SAR until March 2023—almost two years after the conduct began—including due to an extensive delay between escalation of an alert and its subsequent investigation.

7. Customer Group C

Of the missed and improperly reported suspicious transactions identified by FinCEN, roughly 2,000 transactions were processed for Customer Group C, primarily during a nine-month period, from July 2023 to April 2024, with an aggregate value of over $250 million. Customer Group C, purportedly operating in the sales finance and real estate industries, had informed TD Bank, as part of the Bank's CDD processes, that their intended wire activity would be minimal and would not exceed $25,000. Additionally, Customer Group C estimated their annual sales would not exceed $1 million; in fact, Customer Group C conducted over $1 billion in transactions through TD Bank during

the relevant period, with over 90% of the incoming funds from a UK-based cryptocurrency exchange and more than 60% of outgoing transactions sent as wires to a Colombian financial institution that also offers virtual asset-related services.

The pattern of activity revealed Customer Group C conducted, on average, over $100 million in wire transfers each month, most of which facilitated apparent third-party cryptocurrency trading and involved high-risk industries and jurisdictions, including Colombia, China, and countries in the Middle East. Yet this significantly deviated from Customer Group C's onboarding documentation, which did not identify Colombia or China as jurisdictions through which cross-border transactions were expected to be processed. During this time, Customer Group C received more than $650 million from an international cryptocurrency exchange platform, where the purpose, ultimate originators, and source of funds were unknown to TD Bank. Despite this high volume of funds from unknown sources, TD Bank continued to process transactions for Customer Group C, including the facilitation of over $420 million to a financial institution offering cryptocurrency services in the high-risk jurisdiction of Colombia. TD Bank processed these transactions on behalf of Customer Group C, due in part to a lack of clear controls applicable to customers dealing in cryptocurrency: the limited high-level written policies the Bank had in place relating to virtual assets alluded to the requirements for certain additional controls and monitoring. However, there is no evidence any enhanced controls were ever applied to Customer Group C's extensive transactions with virtual asset service providers.

Despite the high volume of suspicious transactions and "red flags" associated with high-risk jurisdictions and rapid movement of funds within a short timeframe, TD Bank failed to proactively report this suspicious activity until it received multiple law enforcement inquiries about Customer Group C. Furthermore, four months after Customer Group C was onboarded by the Bank, a financial regulator ordered an affiliate of Customer Group C to cease its operations, and its assets were ordered

to be liquidated for the benefit of investors. TD Bank failed to conduct appropriate due diligence and only identified this adverse media related to Customer Group C after inquiries from law enforcement.

III. VIOLATIONS

FinCEN determined TD Bank willfully violated the BSA and its implementing regulations during the Relevant Time Period. Specifically, FinCEN determined TD Bank willfully failed to implement and maintain an AML program that met the minimum requirements of the BSA, in violation of 31 U.S.C. § 5318 (h)(1) and 31 C.F.R. § 1020.210(a). Additionally, FinCEN determined TD Bank willfully failed to accurately and timely report suspicious transactions and Currency Transaction Reports to FinCEN, in violation of 31 U.S.C. § 5318(g) and 31 C.F.R. § 1020.320, and 31 U.S.C. § 5313 and 31 C.F.R. § 1010.311, respectively.

IV. ENFORCEMENT FACTORS

As summarized below, FinCEN considered all factors outlined in the Statement on Enforcement of the Bank Secrecy Act issued August 18, 2020, when deciding whether to impose a civil money penalty in this matter.[81]

1. **Nature and seriousness of the violations, including the extent of possible harm to the public and the amounts involved:** TD Bank's violations presented significant risk of serious harm to the U.S. financial system. AML senior management knew that its failure to adequately support AML compliance created backlogs that allowed illicit transactions to continue to be effected through TD Bank and chose to only "gradually reduce" its lengthy queues of alerts and investigations (leading to delayed reporting, account closures, etc.). AML senior management was aware that its piecemeal design and implementation of its transaction monitoring system was

[81] FinCEN, Statement on Enforcement of the Bank Secrecy Act (Aug. 18, 2020).

inadequate and lagging behind its peers, yet adopted an incremental approach to transaction monitoring that caused billions of dollars in illicit funds to flow through the U.S. financial system without effective monitoring. Notably, TD Bank allowed trillions of dollars of domestic ACH, remote deposit capture, and P2P transactions to go unmonitored for over a decade. For example, AML senior management knew this lack of monitoring presented illicit finance risks, specifically with regard to P2P transactions. Similarly, TD Bank improperly discounted money-laundering risks presented by customer relationships involving high-risk jurisdictions, such as Colombia, Cuba, and China. In opening accounts for these high-risk customers, TD Bank did not adequately mitigate risks associated with, among other things, funnel accounts and money laundering. Once accounts were opened and funnel activity was identified, TD Bank knowingly failed to timely mitigate the risks stemming from these flows. Additionally, the Bank failed to timely identify clear indicia of involvement of branch employees in suspicious activity. As a result of these foregoing issues known to AML senior management, TD Bank employees facilitated the movement of substantial sums of illicit funds through the U.S. financial system, including hundreds of millions of dollars related to numerous criminal prosecutions.

2. **Impact or harm of the violations on FinCEN's mission to safeguard the financial system from illicit use, combat money laundering, and promote national security**: As a general matter, SARs represent one of the most important tools to FinCEN and law enforcement in fighting financial crime, both in proactively identifying potential illicit activity and in understanding the scope and scale of that illicit activity. FinCEN and law enforcement must be able to rely on financial institutions to remain vigilant and comply with their obligation to report suspicious activity, and TD Bank's severe underinvestment in personnel, technology, and training caused a significant gap in the identification and reporting of suspicious activity. This

underinvestment persisted despite clear indications that illicit actors were exploiting these deficiencies in order to launder money through the Bank. TD Bank further materially harmed FinCEN's mission to safeguard the U.S. financial system from illicit use because it opened its doors to high-risk customers from jurisdictions posing elevated risks of illicit financial activity without taking requisite steps to account for, and mitigate, the known risks associated with such high-risk customers. Finally, TD Bank not only failed to timely file required reports with FinCEN, but also many of the reports that TD Bank did file were so inaccurate that they were misleading to law enforcement and severely hindered financial crime investigations.

3. **Pervasiveness of wrongdoing within an entity, including management's complicity in, condoning or enabling of, or knowledge of the conduct underlying the violations:** TD Bank's violations were systemic and pervasive. Despite the impact on AML compliance, AML management prioritized "flat cost" budgeting over compliance, only significantly increasing resources late in the Relevant Time Period and largely after the Bank was aware it was under investigation. Despite AML senior management's knowledge of longstanding issues, TD Bank has yet to fully implement an effective automated transaction monitoring system that addresses the Bank's identified money laundering risks. In the face of specific opportunities to mitigate its risks and remediate AML-related issues involving past customers and transactions, AML senior management failed to make necessary investments and acted with unreasonable delay. Moreover, FinCEN's investigation identified instances in which TD Bank's BSA Officer, and other AML senior management, presented unrealistically optimistic forecasts to Bank executives and the Boards.

4. **History of similar violations, or misconduct in general, including prior criminal, civil, and regulatory enforcement actions:** FinCEN's 2013 Consent Order specifically addressed, among

other things, TD Bank's violation of the BSA by failing to file SARs and properly train its AML investigators and staff. Additionally, DOJ indicted several TD Bank customers for allegedly helping to create shell companies and TD Bank employees who opened bank accounts and issued dozens of debit cards, allowing individuals in Colombia to withdraw laundered money.

5. **Financial gain or other benefit resulting from, or attributable to, the violations:** TD Bank incentivized a "flat cost" approach to budgeting, which resulted in an underinvestment in its AML program by substantial sums. During the Relevant Time Period, TD Bank gained an unfair and inappropriate advantage over its peers by spending an order of magnitude less on AML compliance and ignoring clear indications that its AML compliance program was critically lacking. The Bank's fervent emphasis on costs fostered an environment that discouraged addressing the material, substantive AML compliance issues that the Bank faced. Furthermore, AML senior management knew that the Bank was chronically underspending on AML, resulting in an inadequate AML program in violation of BSA requirements. Notably, TD Bank's chronic underinvestment in its transaction monitoring system and its failure to dedicate adequate resources to address its investigations backlogs resulted in thousands of SAR violations related to a host of illicit activity; Bank personnel were aware that suspicious activity was not being timely identified and reported due to these gaps. Nevertheless, the Bank continued to delay technology implementation and investment in personnel, which allowed it to maintain and grow its business without corresponding compliance costs.

6. **Presence or absence of prompt, effective action to terminate the violations upon discovery, including self-initiated remedial measures:** Despite TD Bank's awareness of significant gaps and the corresponding risks in its AML program and impact of the filing of SARs, it nevertheless continued business as usual for more than a decade. TD Bank began to take steps to meaningfully

address these gaps only after coming under scrutiny from regulators and law enforcement years after it identified pervasive issues, such as those involving its transaction monitoring system and backlogs of suspicious activity reviews. For example, the Bank was aware of the heightened risk posed by gaps in its controls related to high-risk jurisdictions and Zelle activity but elected not to pursue strategies to mitigate these risks due to cost and resourcing considerations. Similarly, when presented with opportunities to remediate customers that had not been properly risk-rated, AML senior management elected to take no action to correct such issues and instead turned a blind eye to the relevant risks. While the Bank has begun an extensive remediation plan with interim mitigating controls, there are still outstanding remedial measures that have not been completed by the Bank, such as remedial action for its domestic transaction monitoring gap related to ACH payments and monetary instruments.

7. **Timely and voluntary disclosure of the violations to FinCEN:** TD Bank did not voluntarily disclose all of the issues described above, and FinCEN's investigation was not the result of Bank disclosures.

8. **Quality and extent of cooperation with FinCEN and other relevant agencies, including as to potential wrongdoing by its directors, officers, employees, agents, and counterparties:** TD Bank's cooperation with FinCEN's investigation was generally of a high quality and provided extensive coverage of relevant issues through several tolling agreements, timely and well-organized productions of responsive materials, multiple fact-based presentations, and making available third parties engaged by the Bank to answer FinCEN's questions. However, such cooperation was materially undermined by the Bank failing to timely disclose the ongoing nature of certain issues that persisted late into FinCEN's investigation of TD Bank.

9. **Systemic Nature of the Violations. Considerations include, but are not limited to, the number and extent of violations, failure rates (*e.g.*, the number of violations out of total number of transactions), and duration of violations:** As explained above, the violations that FinCEN identified were numerous, significant in aggregate value, occurred over an extended period, and implicated a broad range of money laundering typologies and resulting harm to the U.S. financial system. TD Bank's consistent underinvestment in its resourcing and transaction monitoring system caused the Bank to not have a fully functional transaction monitoring system for nearly a decade. These failures caused substantial backlogs in alerts for investigation and in the offboarding of customers, which allowed illicit activity to flow through the Bank for extended periods of time. Likewise, for over a decade TD Bank failed to monitor trillions of dollars of domestic transactions including peer-to-peer payments and checks, which caused the Bank to fail to identify and timely report suspicious activity. TD Bank's employees at several branches also systemically failed to report and even facilitated at times various typologies of suspicious activity, as demonstrated by the funnel account activity and Sze network.

10. **Whether another agency took enforcement action for related activity. FinCEN will consider the amount of any fine, penalty, forfeiture, and/or remedial action ordered:** Following separate but parallel investigations, TD Bank has agreed to pay approximately $1.89 billion to DOJ, $123.5 million to the Federal Reserve Board, and $450 million to the OCC to resolve these investigations.

V. CIVIL PENALTY

FinCEN may impose a Civil Money Penalty of up to $69,733 per day for willful violations of the requirement to implement and maintain an AML program.[82]

[82] 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

For each willful violation of a SAR or CTR reporting requirement, FinCEN may impose a civil money penalty not to exceed the greater of the amount of the transaction (capped at $278,937) or $69,733.[83]

After considering all the facts and circumstances, as well as the enforcement factors discussed above, FinCEN is imposing a Civil Money Penalty of $ 1.3 billion in this matter. FinCEN has agreed to credit against the $1.3 billion Civil Money Penalty payments of $543 million to DOJ and the OCC. Accordingly, TD Bank shall make payment of $757 million to the U.S. Department of the Treasury pursuant to the payment instructions that will be transmitted to TD Bank upon execution of this Consent Order.

VI. UNDERTAKINGS

The undertakings agreed to in this Consent Order are in addition to, and independent of, any undertakings to which TD Bank or its affiliates agree in connection with any related consent order or plea agreement, settlement agreement, or any other agreements with or orders imposed by any other representative of the United States or agencies thereof.[84] By execution of this Consent Order, TD Bank agrees to the following Undertakings:

A. INDEPENDENT COMPLIANCE MONITOR

1. TD Bank agrees to retain an independent compliance monitor (Monitor) promptly after FinCEN's selection pursuant to Paragraph 4 below.

2. The Monitor's duties and authority, and the obligations of TD Bank with respect to FinCEN, are set forth in Attachment A, which is incorporated by reference into this Consent Order. TD Bank is responsible for ensuring that the Monitor carries the responsibilities set forth in

[83] 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

[84] Upon request, the OCC may receive copies of all reports referenced in Sections VI.B through VI.E. The transmission of reports from FinCEN's Independent Compliance Monitor selected pursuant to VI.A is described in Attachment A.

Attachment A. Within 30 days after the Effective Date of this Consent Order, TD Bank shall submit a written proposal identifying no less than three candidates to act as Monitor, and, at a minimum, providing the following:

i. a description of each candidate's qualifications and credentials in support of the evaluative considerations and factors listed below;

ii. a written certification by TD Bank that it will not employ, contract with, or otherwise have any affiliation with the Monitor, any member of the Monitor's team, or the Monitor's firm for a period of not less than two years from the date of the termination of the Term of the Monitorship (as defined below);

iii. a written certification by each of the candidates that they are not a current or recent (*i.e.*, within the prior two years) employee, officer, director, agent, or representative of TD Bank and hold no interest in and have no relationship with TD Bank, its subsidiaries, or affiliates or with their respective employees, officers, directors, agents, or representatives.

iv. a written certification by each of the candidates that they have provided notice of their candidacy to any clients that the candidate represents in a matter involving FinCEN, and that the candidate has either obtained a waiver from those clients or has withdrawn as counsel in the other matter(s); and

v. a statement identifying the candidate that is TD Bank's first, second, and third choice to serve as the Monitor.

3. The candidates to act as Monitor or their team members shall have, at a minimum, the following qualifications (Minimum Qualifications):

a. demonstrated expertise with respect to the BSA;

b. experience designing and/or reviewing corporate compliance policies, procedures, and internal controls, including AML-related controls such as transaction monitoring, data governance, customer due diligence, and the independence of compliance personnel from revenue generating units;

c. the ability to access and deploy resources, including the work of outside consultants, to discharge the Monitor's duties as described in this Consent Order; and

d. sufficient independence from TD Bank to ensure effective and impartial performance of the Monitor's duties as described in this Consent Order.

4. FinCEN retains the right, in its exclusive discretion, to choose the Monitor from among the candidates proposed by TD Bank, though TD Bank may express its preference(s) among the candidates. Monitor selections shall be made in keeping with FinCEN's commitment to diversity and inclusion. If FinCEN determines, in its exclusive discretion, that any candidate is not, in fact, qualified to serve as the Monitor, or if FinCEN, in its exclusive discretion, is not satisfied with any candidate proposed, FinCEN reserves the right to reject that candidate. In the event that FinCEN rejects any proposed candidate, TD Bank shall propose additional candidates within 30 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, unless FinCEN, at any time and in its sole discretion, determines that TD Bank is not recommending candidates in good faith. If FinCEN makes such a determination, FinCEN may solicit applications from the public and select a Monitor from among those applicants meeting the Minimum Qualifications. FinCEN will endeavor to complete the selection process within 60 days of the execution of this Consent Order. If the Monitor resigns or is otherwise unable to fulfill their obligations as set out herein and in Attachment A, TD

Bank shall within 20 days recommend a pool of three qualified candidates from which FinCEN will choose a replacement through the process set out herein.

5. The Monitor's term shall be four years from the date on which the Monitor is retained by TD Bank (Term of the Monitorship). The Monitor shall be retained at TD Bank's own expense throughout the Term of the Monitorship. In the event that FinCEN finds, in its exclusive discretion, that there exists a change in circumstances sufficient to eliminate the need for the Monitor, and that the other provisions of this Consent Order have been satisfied, the Term of the Monitorship may be terminated early. Without prejudice to FinCEN's right to proceed in the event of a Breach of this Consent Order, FinCEN may, in consultation with the Monitor extend the Term for up to a total additional time of one year.

6. The Monitor's powers, duties, and responsibilities, as well as additional circumstances that may support an extension of the Monitor's term or its early termination, are set forth in Attachment A. TD Bank agrees that it will not employ, contract with, or otherwise be affiliated with the Monitor or the Monitor's firm for a period of not less than two years from the date on which the Monitor's term expires. Nor will TD Bank discuss with the Monitor, any member of the Monitor's team, or the Monitor's firm the possibility of further employment or affiliation at any time during the Term of the Monitorship and for a period of two years after the Monitor's term expires.

7. TD Bank agrees to require that its wholly owned subsidiaries and affiliates comply with the requirements and obligations set forth in Attachment A, provided that compliance with such requirements and obligations would not violate locally applicable laws and regulations or the instructions of local regulatory agencies.

B. SAR LOOKBACK UNDERTAKING

8. In connection with this resolution, TD Bank has engaged a qualified independent consultant (SAR Lookback Consultant)[85] at its own expense, to conduct a SAR Lookback Review. The scope of the SAR Lookback Consultant's work, including but not limited to the SAR Lookback Review, will be evaluated and overseen by the Monitor. The SAR Lookback Consultant will determine whether activity effected by TD Bank's customers, from 2018 until the completion of TD Bank's phased implementation of its new transaction monitoring system,[86] is properly identified and reported under 31 U.S.C. § 5318(g) and implementing regulations, including but not limited to: (i) transactions effected via Zelle and other P2P payment products, (ii) transactions involving or related to high-risk jurisdictions, including transactions consistent with funnel account typologies, and (iii) transactions that did not generate an alert due to gaps in the coverage of TD Bank's automated monitoring system, such as gaps related to coverage of ACH and RDC transactions, as well as gaps stemming from TD Bank's failures to implement new scenarios during the Relevant Time Period, resume scenarios that had been temporarily paused, or to capture other types of transactions (Covered Transactions).

9. Within 150 days from the date of engagement of the Monitor, the SAR Lookback Consultant will deliver to FinCEN and the Monitor a report summarizing the proposed scope and methodology of the review of the Covered Transactions that the SAR Lookback Consultant plans to conduct (SAR Lookback Scope Report). FinCEN, in consultation with the Monitor, may amend the

[85] Upon selection of the Monitor, the Monitor will review the terms of the Bank's engagement of the SAR Lookback Consultant, and as appropriate, require the Bank to revise the engagement to comply with the requirements of FinCEN's SAR Lookback Review.

[86] Covered Transactions in the SAR Lookback Review will include transactions not subject to automated monitoring by the Bank's new transaction monitoring system during the phased implementation of this system. In determining the appropriate scope and methodology applicable to such Covered Transactions, the SAR Lookback Consultant and the Monitor may consider the Bank's use of compensating controls prior to the completed implementation of the new transaction monitoring system.

scope of the review of Covered Transactions within 30 days of FinCEN's receipt of the report summarizing the proposed scope and methodology. Following submission of the SAR Lookback Scope Report to FinCEN, the SAR Lookback Consultant will deliver quarterly progress reports to the Monitor documenting the status of the SAR Lookback Review. Based on the quarterly progress reports, FinCEN, in consultation with the Monitor, may expand the time period of the SAR Lookback Review within the Relevant Time Period.

10. Within eighteen months from the date of the SAR Lookback Scope Report, and no later than April 2027, the SAR Lookback Consultant will deliver a detailed report (SAR Lookback Report) to FinCEN, the Monitor, and TD Bank that summarizes the methodology and findings of its review and identifies the Covered Transactions that may require a SAR to be filed pursuant to 31 U.S.C. § 5318(g) and its implementing regulations. TD Bank will make, and will cause the SAR Lookback Consultant to make, interim reports, drafts, work papers, or other supporting materials related to the SAR Lookback Review available to FinCEN upon request. TD Bank will comply with the findings of the SAR Lookback Consultant, the Monitor, or FinCEN that TD Bank file SARs on any of the Covered Transactions, and, in the event that any of the SAR Lookback Consultant, the Monitor, or FinCEN recommend that TD Bank file a SAR on a Covered Transaction, TD Bank will comply with that recommendation. TD Bank may begin filing SARs on the Covered Transactions during the pendency of the SAR Lookback Review (and prior to completion of the SAR Lookback Report), provided that the Bank notifies FinCEN at least 30 days prior to commencing such SAR filings.

11. No later than 90 days from the date of the SAR Lookback Report, TD Bank will complete the filing with FinCEN of SARs regarding all the Covered Transactions identified by the independent consultant as ones that would have required a report pursuant to 31 U.S.C. § 5318(g) and implementing regulations. TD Bank shall be entitled to one 60-day extension of this SAR filing deadline as of right. Any additional extensions require the written consent of FinCEN in its sole discretion.

C. AML PROGRAM UNDERTAKING

12. Within 60 days from the date of retention of the Monitor, the Monitor will propose a qualified independent consultant (AML Program Consultant) for TD Bank to hire, at its own expense, to conduct a review of the effectiveness of TD Bank's AML program though an AML Program Review.[87] The Monitor has the right to veto the engagement of an AML Program Consultant that the Monitor deems unsuitable to complete the AML Program Review. The AML Program Review will determine whether TD Bank complies with the BSA.

13. Within 90 days from the date of TD Bank's retention of the AML Program Consultant, the AML Program Consultant will provide FinCEN with a report summarizing the proposed scope and methodology of the review of TD Bank's AML program (AML Program Scope Report). The AML Program Scope Report must include proposed analyses to cover at least the following aspects of TD Bank's AML Program:

i. High-level Commitment to Compliance: the extent to which TD Bank's senior management and, if applicable, directors provide sufficiently strong, explicit, and visible support and commitment to TD Bank's AML program, including the rigor of adherence demonstrated through example, as well as reinforcement by all levels of management

[87] Subject to FinCEN approval, the Monitor may elect to serve as the AML Program Consultant.

within TD Bank to create and foster a culture of ethics and compliance throughout the organization.

ii. Periodic Risk Assessments: the extent to which TD Bank's AML program includes regular, periodic assessments of TD Bank's money laundering, terrorist financing, and other illicit financial activity risks based on TD Bank's business activities, including products, services, distribution channels, customers, intermediaries, and geographic locations.

iii. Policies, Procedures, and Internal Controls: the extent to which TD Bank maintains and enforces clearly articulated and visible corporate AML policies that are consistent with the BSA and applicable to all officers and employees, and, where necessary and appropriate, TD Bank's agents; such policies and related procedures and internal controls shall address, at a minimum:

a. verifying customer identification and know-your-customer (KYC), including the consistent application of proof of address requirements, and the use of customer identification, KYC information, and other data housed by TD Bank to identify users residing in high-risk jurisdictions;

b. transaction monitoring, including the sufficiency of required resources, related data governance controls, and product coverage, such as ACH and RDC transactions, P2P payment services, and trade finance offerings;

c. identifying suspicious activity and filing reports of such activity with FinCEN, including the sufficiency of required resources to identify and report such activity, as well as controls specifically tailored to the risk of employee involvement in such suspicious activity;

d. reporting currency transactions, including coverage of all methods by which TD Bank customers can effect such transactions as well as controls to ensure that all conductors of a given transaction are properly identified by Bank personnel and included in reports to FinCEN;

e. governance structures and processes related to the involvement and stature of AML compliance personnel in decisions related to the launch of new products, services, or channels, as well as material changes that TD Bank makes to its products, services, or channels;

f. restricting or offboarding of customers—including the extent to which personnel from TD Bank's revenue generating units influence the application of such controls, the timeliness of TD Bank's offboarding of customers recommended for exit by AML compliance due to money laundering or terrorist-financing-related risks (including the extent of any delays caused by a lack of resourcing to support such efforts), and the effectiveness of mitigating controls for customers awaiting exit or who have raised money laundering- or terrorist financing-related concerns that TD Bank deems insufficient to require an exit of the relevant account(s);

g. responding to requests for information from law enforcement, regulators, and supervisors; and

h. creating and retaining other records and filing other reports, including identifying mechanisms to inform the board of directors or a committee thereof and senior management of BSA compliance initiatives, identified

compliance deficiencies and corrective actions taken, and notify the board of directors of SARs filed.

iv. Independence, Resourcing, and Empowerment of Compliance: whether TD Bank has assigned responsibility to an individual for assurance of its day-to-day AML program, and the extent of autonomy that individual has from management—as demonstrated by TD Bank's governance structures, the sufficiency of resources, and authority, including with respect to incurring costs to assure compliance with the BSA—to maintain such autonomy.

v. Guidance and Training: the extent to which TD Bank maintains mechanisms to provide periodic training for all TD Bank personnel—including training tailored to TD Bank's money laundering and terrorist financing risks and the recipients' roles, responsibilities, and geographic location within TD Bank, as well as training that incorporates, as permissible under applicable law, TD Bank's prior compliance failures—and records of successful completion of such training.

vi. Internal Reporting and Related Investigations: the extent to which TD Bank maintains an effective system for internal, and, where possible, confidential reporting by, as well as protection of, employees, officers, and where appropriate, agents, concerning violations of AML laws, including through the implementation of mechanisms designed to ensure that the system for such reporting is effectively communicated to all potential reporters and that TD Bank maintains an effective and reliable process with sufficient resources to respond to, investigate, and document the investigation of any such reports.

vii. Enforcement, Discipline, and Employee Compensation: the extent to which TD Bank maintains mechanisms designed to effectively enforce its AML program, including to identify both specific instances of and patterns or trends in employee involvement in suspicious transactions effected by customers, as well as to discipline violations and incentivize compliance by implementing policies, procedures, and internal controls to take reasonable steps to remedy harm stemming from misconduct (which may include updates to the AML program's policies, procedures, and internal controls) and implementing evaluation criteria in its personnel review process to account for actions taken by personnel to ensure compliance with the AML program.

viii. Independent Testing: whether TD Bank conducts periodic reviews and tests of its AML program designed to evaluate and improve its effectiveness in preventing and detecting money laundering, terrorist financing, and other illicit finance activity, including by taking into account ongoing or recently completed enhancements to AML-related systems.

14. FinCEN, in consultation with the Monitor, may amend the scope of the review of TD Bank's AML program through a notification to the Monitor within 30 days of FinCEN's receipt of the report summarizing the proposed scope and methodology. Following submission of the AML Program Scope Report to FinCEN, the Monitor will deliver quarterly progress reports to FinCEN documenting the status of the AML Program Review.

15. Within 60 days from the end of its review, but no later than one year from the date of its engagement, the AML Program Consultant will submit to FinCEN a written report: (i) addressing the adequacy of TD Bank's AML program, including, but not limited to, the areas set forth in the AML Program Scope Report; (ii) describing the review performed; and (iii) describing any

recommended modifications or enhancements to TD Bank's AML program. TD Bank will make, and will cause the AML Program Consultant to make, interim reports, drafts, workpapers, or other supporting materials related to the AML Program Review available to FinCEN upon request.

16. TD Bank, in consultation with the Monitor, will develop a plan to implement any recommendations made in connection with the AML Program Review (Implementation Plan) or, within 90 days after issuance of a report, propose alternatives. The AML Program Consultant will provide a written response to any proposed alternatives within 60 days. Within 180 days after finalization of the Implementation Plan, TD Bank will provide FinCEN and the Monitor with a written report detailing the extent to which it has adopted and implemented the Implementation Plan. As set forth in Attachment A, TD Bank's implementation of the recommendations shall be subject to the Monitor's validation reviews.

D. ACCOUNTABILITY FOR EMPLOYEES INVOLVED IN BSA VIOLATIONS AND RELATED MISCONDUCT

17. The Monitor shall, in addition to other duties described herein, oversee a Third-Party Accountability Review.[88] The Accountability Review process will assess the accountability review work the Bank has conducted prior to the selection of the Monitor concerning the involvement or failure to escalate by current and former TD Bank personnel in conjunction with the conduct described in the Statement of Facts relating to TD Bank's transaction monitoring failures; at the Monitor's discretion, the Accountability Review may also review certain other conduct described in the Statement of Facts, provided that such additional conduct is not covered by TD Bank's completed investigations involving the Sze network and Customer Group A.

[88] Subject to FinCEN approval, the Monitor may elect to propose a qualified independent consultant to assist with the Accountability Review (Accountability Review Consultant).

18. The Accountability Review will assess TD Bank's internal review of the relevant conduct, including both fact-finding and conclusions, undertaken prior to the Monitor's selection. The Monitor may reasonably rely on facts developed pursuant to such internal review. If the Monitor, in their discretion, determines that incremental fact-finding is appropriate, TD Bank shall cooperate with such incremental fact-finding in a manner consistent with its obligations to comply with the Monitor as set forth in Attachment A. The Monitor shall make corresponding recommendations, including consideration of: (i) for current TD Bank employees, potential disciplinary measures; (ii) for former TD Bank employees, recommendations regarding the Bank's potential "clawback" of prior compensation from such employees; and (iii) the culture of compliance at the Bank, including the extent to which such culture of compliance contributed to employee involvement in the Bank's BSA violations and related misconduct.

19. Within 120 days from the date of TD Bank's retention of the Monitor, the Monitor will provide FinCEN with a report summarizing the proposed scope and methodology of the Accountability Review, including the extent to which the Monitor plans to undertake incremental fact-finding. The Monitor will deliver quarterly progress reports to FinCEN documenting the status of the Accountability Review.

20. Within 60 days from the end of its review, but no later than one year from the date of its engagement, the Monitor will submit to FinCEN a written report, including: (i) the Monitor's recommendations and any decisions by the Bank as to whether to continue to retain in the future, directly or indirectly, any officer, employee, agent, consultant, contractor of TD Bank or any affiliate of TD Bank, or in any other capacity individuals who, based on the Accountability Review, participated in the conduct underlying this Consent Order, (ii) formal disciplinary action taken by TD Bank in connection with the conduct described, and (iii) the Monitor's recommendations and any

actions taken by the Bank to strengthen its culture of compliance, including the prioritization, stature, and authority for AML/CFT compliance functions within the Bank, and the level of support for such functions from the Bank's senior management. FinCEN reserves the right to take further action related to current or former TD Bank employees irrespective of their inclusion in the Accountability Review.

E. DATA GOVERNANCE REVIEW OF BSA/AML-RELATED INFORMATION

21. The Monitor shall, in addition to other duties described herein, oversee a Third-Party Data Governance Review.[89] The Data Governance Review will assess the Bank's data governance framework (including implementing policies, procedures, and internal controls) applicable to information that the Bank uses or is otherwise required for use in its AML Program, including but not limited to information related to transaction monitoring for compliance with the Bank's obligation to identify and report suspicious transactions and the Bank's information sharing-related obligations under 31 C.F.R. § 1010.520–540.

22. The Data Governance Review will assess TD Bank's data governance framework for accuracy, completeness, consistency, effectiveness, and timeliness of TD Bank's AML data processing, including relative to TD Bank's size, complexity, and risk profile. The Monitor shall review and make corresponding recommendations, including consideration of TD Bank's: (i) governing bodies, fora, and other structures responsible for the design, implementation, and oversight of the relevant policies, procedures, and internal controls; (ii) identification and definition of relevant stakeholders and their corresponding roles and responsibilities, including the maintenance of Bank personnel with the requisite subject matter expertise applicable to the in-scope data populations; (iii) identification and flow of relevant data sources and associated systems; and

[89] Subject to FinCEN approval, the Monitor may elect to propose a qualified independent consultant to assist with the Data Governance Review (Data Governance Review Consultant), including the AML Program Review Consultant.

(iv) controls and monitoring of the use of relevant data within its AML Program—both as currently designed and with respect to processes governing change- or issue-management—including quality control, assurance, and other error detection mechanisms.

23. Within 120 days from the date of TD Bank's retention of the Monitor, the Monitor will provide FinCEN with a report summarizing the proposed scope and methodology of the Data Governance Review. The Monitor will deliver quarterly progress reports to FinCEN documenting the status of the Data Governance Review.

24. Within 60 days from the end of its review, but no later than one year from the date of its engagement, the Monitor will submit to FinCEN a written report setting forth the Monitor's recommendations and completed remedial actions as well as commitments by TD Bank to revise the Bank's data governance framework.

VII. CONSENT AND ADMISSIONS

To resolve this matter and only for that purpose, TD Bank admits to the Statement of Facts and Violations set forth in this Consent Order to the extent described above and admits that it willfully violated the BSA and its implementing regulations. TD Bank consents to the use of the Statement of Facts, and any other findings, determinations, and conclusions of law set forth in this Consent Order in any other proceeding brought by or on behalf of FinCEN, or to which FinCEN is a party or claimant, and agrees they shall be taken as true and correct and be given preclusive effect without any further proof. TD Bank understands and agrees that in any administrative or judicial proceeding brought by or on behalf of FinCEN against it, including any proceeding to enforce the Civil Money Penalty imposed by this Consent Order or for any equitable remedies under the BSA, TD Bank shall be precluded from disputing any fact or contesting any determinations set forth in this Consent Order.

To resolve this matter, TD Bank agrees to and consents to the issuance of this Consent Order and all terms herein and agrees to make payment of $757 million to the U.S. Department of the Treasury within ten days of the Effective Date of this Consent Order. If timely payment is not made, TD Bank agrees that interest, penalties, and administrative costs will accrue.[90]

TD Bank understands and agrees that it must treat the Civil Money Penalty paid under this Consent Order as a penalty paid to the government and may not claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for any payments made to satisfy the Civil Money Penalty. TD Bank understands and agrees that any acceptance by or on behalf of FinCEN of any partial payment of the Civil Money Penalty obligation will not be deemed a waiver of TD Bank's obligation to make further payments pursuant to this Consent Order, or a waiver of FinCEN's right to seek to compel payment of any amount assessed under the terms of this Consent Order, including any applicable interest, penalties, or other administrative costs.

TD Bank affirms that it agrees to and approves this Consent Order and all terms herein freely and voluntarily and that no offers, promises, or inducements of any nature whatsoever have been made by FinCEN or any employee, agent, or representative of FinCEN to induce TD Bank to agree to or approve this Consent Order, except as specified in this Consent Order.

TD Bank understands and agrees that this Consent Order implements and embodies the entire agreement between TD Bank and FinCEN, and its terms relate only to this enforcement matter and any related proceeding and the facts and determinations contained herein. TD Bank further understands and agrees that there are no express or implied promises, representations, or agreements between TD Bank and FinCEN other than those expressly set forth or referred to in this Consent

[90] 31 U.S.C. § 3717; 31 C.F.R. § 901.9.

Order and that nothing in this Consent Order is binding on any other law enforcement or regulatory agency or any other governmental authority, whether foreign, Federal, State, or local.

TD Bank understands and agrees that nothing in this Consent Order may be construed as allowing TD Bank, its subsidiaries, affiliates, Board, officers, employees, or agents to violate any law, rule, or regulation.

TD Bank consents to the continued jurisdiction of the courts of the United States over it and waives any defense based on lack of personal jurisdiction or improper venue in any action to enforce the terms and conditions of this Consent Order or for any other purpose relevant to this enforcement action. Solely in connection with an action filed by or on behalf of FinCEN to enforce this Consent Order or for any other purpose relevant to this action, TD Bank authorizes and agrees to accept all service of process and filings through the Notification procedures below and to waive formal service of process.

VIII. COOPERATION

TD Bank shall fully cooperate with FinCEN in any and all matters within the scope of or related to the Statement of Facts, including any investigation of its current or former directors, officers, employees, agents, consultants, or any other party. TD Bank understands its cooperation pursuant to this paragraph shall include, but is not limited to, truthfully disclosing all factual information with respect to its activities, and those of its present and former directors, officers, employees, agents, and consultants. This obligation includes providing to FinCEN, upon request, any document, record, or other tangible evidence about which FinCEN may inquire of TD Bank. TD Bank's cooperation pursuant to this paragraph is subject to applicable laws and regulations, as well as valid and properly documented claims of attorney-client privilege or the attorney work product doctrine.

IX. RELEASE

Execution of this Consent Order and compliance with all of the terms of this Consent Order settles all claims FinCEN may have against TD Bank for the conduct described in this Consent Order during the Relevant Time Period. Execution of this Consent Order, and compliance with the terms of this Consent Order, does not release any claim FinCEN may have for conduct by TD Bank other than the conduct described in this Consent Order during the Relevant Time Period, or any claim FinCEN may have against any current or former director, officer, owner, or employee of TD Bank or any other individual or entity other than those named in this Consent Order. In addition, this Consent Order does not release any claim or provide any other protection in any investigation, enforcement action, penalty assessment, or injunction relating to any conduct after the Relevant Time Period as described in this Consent Order.

X. WAIVERS

Nothing in this Consent Order shall preclude any proceedings brought by, or on behalf of, FinCEN to enforce the terms of this Consent Order, nor shall it constitute a waiver of any right, power, or authority of any other representative of the United States or agencies thereof, including but not limited to DOJ.

In consenting to and approving this Consent Order, TD Bank stipulates to the terms of this Consent Order and waives:

A. Any and all defenses to this Consent Order, the Civil Money Penalty imposed by this Consent Order, and any action taken by or on behalf of FinCEN that can be waived, including any statute of limitations or other defense based on the passage of time;

B. Any and all claims that FinCEN lacks jurisdiction over all matters set forth in this Consent Order, lacks the authority to issue this Consent Order or to impose the Civil Money

Penalty, or lacks authority for any other action or proceeding related to the matters set forth in this Consent Order;

C. Any and all claims that this Consent Order, any term of this Consent Order, the Civil Money Penalty, or compliance with this Consent Order or the Civil Money Penalty, is in any way unlawful or violates the Constitution of the United States of America or any provision thereof;

D. Any and all rights to judicial review, appeal or reconsideration, or to seek in any way to contest the validity of this Consent Order, any term of this Consent Order, or the Civil Money Penalty arising from this Consent Order;

E. Any and all claims that this Consent Order does not have full force and effect, or cannot be enforced in any proceeding, due to changed circumstances, including any change in law; and

F. Any and all claims for fees, costs, or expenses related in any way to this enforcement matter, Consent Order, or any related administative action, whether arising under common law or under the terms of any statute, including, but not limited to, under the Equal Access to Justice Act. TD Bank agrees to bear its own costs and attorneys' fees.

XI. VIOLATIONS OF THIS CONSENT ORDER

Determination of whether TD Bank has failed to comply with this Consent Order, or any portion thereof, and whether to pursue any further action or relief against TD Bank shall be in FinCEN's sole discretion. If FinCEN determines, in its sole discretion, a failure to comply with this Consent Order, or any portion thereof, has occurred, or TD Bank made any misrepresentations to FinCEN or any other government agency related to the underlying enforcement matter, FinCEN may void any and all releases or waivers contained in this Consent Order; reinstitute administrative

proceedings; take any additional action it deems appropriate; and pursue any and all violations, maximum penalties, injunctive relief, or other relief FinCEN deems appropriate. FinCEN may take any such action even if it did not take such action against TD Bank in this Consent Order and notwithstanding the releases and waivers herein. In the event FinCEN takes such action under this paragraph, TD Bank expressly agrees to toll any applicable statute of limitations and to waive any defenses based on a statute of limitations or the passage of time applicable to the Statement of Facts in this Consent Order, until a date 180 days following TD Bank's receipt of notice of FinCEN's determination that a misrepresentation or breach of this agreement has occurred, except as to claims already time barred as of the Effective Date of this Consent Order.

In the event that FinCEN determines that TD Bank has made a misrepresentation or failed to comply with this Consent Order, or any portion thereof, all statements made by or on behalf of TD Bank to FinCEN, including the Statement of Facts, whether prior or subsequent to this Consent Order, will be admissible in evidence in any and all proceedings brought by or on behalf of FinCEN. TD Bank agrees that it will not assert any claim under the Constitution of the United States of America, Rule 408 of the Federal Rules of Evidence, or any other law or federal rule that any such statements should be suppressed or are otherwise inadmissible. Such statements shall be treated as binding admissions, and TD Bank agrees that it shall be precluded from disputing or contesting any such statements. FinCEN shall have sole discretion over the decision to impute conduct or statements of any director, officer, employee, agent, or any person or entity acting on behalf of, or at the direction of TD Bank in determining whether TD Bank has violated any provision of this Consent Order.

XII. PUBLIC STATEMENTS

TD Bank agrees it shall not, nor shall its attorneys, agents, partners, directors, officers, employees, affiliates, or any other person authorized to speak on its behalf or within its authority or

control, take any action or make any public statement, directly or indirectly, contradicting its admissions and acceptance of responsibility or any terms of this Consent Order, including any fact finding, determination, or conclusion of law in this Consent Order.

FinCEN shall have sole discretion to determine whether any action or statement made by TD Bank, or by any person under the authority, control, or speaking on behalf of TD Bank contradicts this Consent Order, and whether TD Bank has repudiated such statement.

XIII. RECORD RETENTION

In addition to any other record retention required under applicable law, TD Bank agrees to retain all documents and records required to be prepared or recorded under this Consent Order or otherwise necessary to demonstrate full compliance with each provision of this Consent Order, including supporting data and documentation. TD Bank agrees to retain these records for a period of 6 years after creation of the record, unless required to retain them for a longer period of time under applicable law.

XIV. SEVERABILITY

TD Bank agrees that if a court of competent jurisdiction considers any of the provisions of this Consent Order unenforceable, such unenforceability does not render the entire Consent Order unenforceable. Rather, the entire Consent Order will be construed as if not containing the particular unenforceable provision(s), and the rights and obligations of FinCEN and TD Bank shall be construed and enforced accordingly.

XV. SUCCESSORS AND ASSIGNS

TD Bank agrees that the provisions of this Consent Order are binding on its owners, officers, employees, agents, representatives, affiliates, successors, assigns, and transferees to whom TD Bank agrees to provide a copy of the executed Consent Order. Should TD Bank seek to sell, merge, transfer,

or assign its operations, or any portion thereof, that are the subject of this Consent Order, TD Bank must, as a condition of sale, merger, transfer, or assignment obtain the written agreement of the buyer, merging entity, transferee, or assignee to comply with this Consent Order.

XVI. MODIFICATIONS AND HEADINGS

This Consent Order can only be modified with the express written consent of FinCEN and TD Bank. The headings in this Consent Order are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Order or its individual terms.

XVII. AUTHORIZED REPRESENTATIVE

TD Bank's representative, by consenting to and approving this Consent Order, hereby represents and warrants that the representative has full power and authority to consent to and approve this Consent Order for and on behalf of TD Bank and further represents and warrants that TD Bank agrees to be bound by the terms and conditions of this Consent Order.

XVIII. NOTIFICATION

Unless otherwise specified herein, whenever notifications, submissions, or communications are required by this Consent Order, they shall be made in writing and sent via first-class mail and simultaneous email, addressed as follows:

To FinCEN:

Associate Director, Enforcement and Compliance Division
Financial Crimes Enforcement Network
P.O. Box 39, Vienna, Virginia 22183

To TD Bank, N.A. and TD Bank USA, N.A.:

General Counsel
TD Bank
1 Vanderbilt Avenue, 14th Floor, New York, New York 10017

Notices submitted pursuant to this paragraph will be deemed effective upon receipt unless otherwise provided in this Consent Order or approved by FinCEN in writing.

XIX. COUNTERPARTS

This Consent Order may be signed in counterpart and electronically. Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

XX. EFFECTIVE DATE AND CALCULATION OF TIME

This Consent Order shall be effective upon the date signed by FinCEN. Calculation of deadlines and other time limitations set forth herein shall run from the effective date (excluding the effective date in the calculation) and be based on calendar days, unless otherwise noted, including intermediate Saturdays, Sundays, and legal holidays.

By Order of the Director of the Financial Crimes Enforcement Network.

/s/
Andrea Gacki Date:
Director

Consented to and Approved By:

/s/
Cynthia Adams Date:
TD Bank, N.A. and TD Bank USA, N.A.

ATTACHMENT A

INDEPENDENT COMPLIANCE MONITOR

The duties and authority of the Monitor, and the obligations of TD Bank, on behalf of itself, its subsidiaries, and its affiliates, with respect to the Monitor and FinCEN, are as described below:

1. TD Bank shall retain the Monitor for a period of four years (the Term of the Monitorship), unless the early termination or extension provisions of Paragraph 4 of Section VII.A of the Consent Order is triggered.

Monitor's Mandate

2. The Monitor's primary responsibility is, in the manner set forth below, to: (i) assess and monitor TD Bank's compliance with the terms of the Consent Order, including completion of the Undertakings set forth in Section VI, so as to specifically address and reduce the risk of any recurrence of TD Bank's misconduct; (ii) evaluate the effectiveness of TD Bank's compliance with the BSA and implementing regulations; and (iii) assess and monitor senior management's commitment to and effective implementation of TD Bank's AML compliance program (collectively, the Mandate).

TD Bank's Obligations

3. TD Bank shall cooperate fully with the Monitor, and the Monitor shall have the authority to take such steps as, in their view, may be reasonably necessary to be fully informed about TD Bank's AML compliance program in accordance with the terms of the Consent Order and the animating principles thereof, subject to applicable law, including applicable data protection and labor laws and regulations. To that end, TD Bank shall: facilitate the Monitor's access to TD Bank's documents and resources; not limit such access, except as provided in

Paragraphs 4–5; and provide guidance on applicable local law (such as relevant data protection and labor laws). TD Bank shall provide the Monitor with access to all information, documents, records, facilities, and employees, as requested by the Monitor, that fall within the scope of the Mandate of the Monitor under the Consent Order and this Attachment A. TD Bank shall use its best efforts to provide the Monitor with access to TD Bank's former employees and its third-party vendors, agents, consultants, contractors, and subcontractors.

Withholding Access

4. The parties agree that no attorney-client relationship shall be formed between TD Bank and the Monitor. In the event that TD Bank seeks to withhold from the Monitor access to information, documents, records, facilities, or current or former employees of TD Bank that may be subject to a claim of attorney-client privilege or to the attorney work-product doctrine, or where TD Bank reasonably believes production would otherwise be inconsistent with applicable law or regulation, TD Bank shall work cooperatively with the Monitor to resolve the matter to the satisfaction of the Monitor.

5. If the matter cannot be resolved, at the request of the Monitor, TD Bank shall promptly provide written notice to the Monitor and FinCEN. Such notice shall include a general description of the nature of the information, documents, records, facilities, or current or former employees that are being withheld, as well as the legal basis for withholding access. FinCEN reserves the right to seek to compel access to such information, documents, records, facilities, or employees.

Monitor's Coordination with TD Bank and Review Methodology

6. In carrying out the Mandate, to the extent appropriate under the circumstances, the Monitor should coordinate with TD Bank's personnel, including in-house counsel, compliance

personnel, internal auditors, and the SAR Lookback and AML Program Consultants engaged to complete the SAR Lookback and AML Program Reviews set forth in Sections VI.B and VI.C, respectively, of the Consent Order on an ongoing basis. In carrying out the Mandate, the Monitor shall propose the selection of the AML Program Consultant and review the Bank's engagement of the SAR Lookback Consultant, and maintain the right to veto the engagement of a proposed independent consultant that the Monitor deems unsuitable to complete the SAR Lookback and AML Program Reviews.[91] The Monitor may rely on the product of TD Bank's processes, including but not limited to studies, reviews, sampling and testing methodologies, audits, and analyses conducted by or on behalf of TD Bank, as well as TD Bank's internal resources (*e.g.*, legal, compliance, and internal audit), which can assist the Monitor in carrying out the Mandate, provided that the Monitor has confidence in the quality of those resources. In this regard, the Monitor may consider the SAR Lookback and AML Program Reviews, as well as any other independent consultants that TD Bank voluntarily engages to assist in its compliance with the BSA.

7. Subject to the specific requirements set forth in Sections VI.B and VI.C of the Consent Order to oversee the SAR Lookback and AML Program Reviews, the Monitor's reviews should use a risk-based approach, and thus, the Monitor 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: (i) the particular markets in which TD Bank offers its products and services, including the locations of TD Bank's customers; (ii) the types of products and services that TD Bank offers its customers; (iii) the status

[91] Subject to FinCEN approval, the Monitor may elect to conduct either one or both of the SAR Lookback Review and AML Program Review.

and strength of TD Bank's controls to identify and report suspicious transactions; (iv) the customer identification and verification policies applied to TD Bank's customers; (v) the number, type, and frequency of alerts that have been triggered by types or groups of customers and how TD Bank has handled those alerts; (vi) the sufficiency of the AML-related personnel and resources within the compliance function; and (vii) the status and strength of TD Bank's geofencing controls, including to identify TD Bank customers effecting transactions in high-risk jurisdictions.

8. In undertaking the reviews described below to carry out the Mandate, the Monitor shall formulate conclusions based on, among other things: (a) inspection of relevant documents, including TD Bank's current policies and procedures; (b) on-site observation of selected systems and procedures of TD Bank at sample sites, including transaction monitoring, record-keeping, and internal audit procedures; (c) meetings with and interviews of relevant current and, where appropriate, former directors, officers, employees, business partners, agents, and other persons at mutually convenient times and places; and (d) the SAR Lookback and AML Program Reviews.

Monitor's Written Work Plans

9. To carry out the Mandate, during the Term of the Monitorship, the Monitor shall conduct an initial scoping review (First Review) and prepare a first report (First Report), followed by at least four follow-up reviews and reports as described in Paragraphs 12–17 below. With respect to the First Report, after consultation with TD Bank and FinCEN, the Monitor shall prepare the first written work plan within 60 days of being retained, and TD Bank and FinCEN shall provide comments within 30 days of receipt of the written work plan. The first written work plan must describe the proposed parameters, high-level timelines, and key dependencies associated with the SAR Lookback and AML Program Reviews, including the scope of such undertakings and the Monitor's proposed oversight of the SAR Lookback and AML Program Consultants. With

respect to each follow-up report, after consultation with TD Bank and FinCEN, the Monitor shall prepare a written work plan at least 30 days prior to commencing a review, and TD Bank and FinCEN shall provide comments within 20 days after receipt of the written work plan. Any disputes between TD Bank and the Monitor with respect to any written work plan shall be decided by FinCEN in its exclusive discretion.

10. All written work plans shall identify with reasonable specificity the activities the Monitor plans to undertake in execution of the Mandate, including a written request for documents, as applicable. The Monitor's work plan for the first review shall include such steps as are reasonably necessary to conduct an effective first review in accordance with the Mandate, including by: (i) developing an understanding, to the extent the Monitor deems appropriate, of the facts and circumstances surrounding any violations of the BSA that occurred before the date of the Consent Order; and (ii) using that understanding to recommend changes to the scope of the SAR Lookback and AML Program Reviews. In developing an understanding of TD Bank's historical violations of the BSA, the Monitor is to rely, to the extent possible, on available information and documents provided by TD Bank. The Monitor need not conduct its own inquiry into the historical events that gave rise to the Consent Order except as otherwise necessary to fulfill the Mandate.

First Review

11. The First Review shall commence no later than 90 days from the date of the engagement of the Monitor (unless otherwise agreed by FinCEN). The Monitor shall issue a written report (First Report) within 90 days of commencing the first review, setting forth: (i) the scope of the AML Program and SAR Lookback Reviews, including applicable requirements set forth in Sections VI.B and VI.C of the Consent Order; and (ii) any other work designed to enhance

TD Bank's program for ensuring compliance with the BSA. The Monitor should consult with TD Bank concerning the Monitor's findings and recommendations on an ongoing basis and should consider TD Bank's comments and input to the extent the Monitor deems appropriate. The Monitor may also choose to share a draft of their reports with TD Bank prior to finalizing them. The Monitor's reports need not recite or describe comprehensively TD Bank's history or compliance policies, procedures, and practices, but rather may focus on those areas with respect to which the Monitor wishes to make recommendations, if any, for improvement or which the Monitor otherwise concludes merit particular attention. The Monitor shall provide its reports to TD Bank senior management and contemporaneously transmit copies to:

Associate Director, Enforcement and Compliance Division
Financial Crimes Enforcement Network
P.O. Box 39, Vienna, Virginia 22183

Examiner-in-Charge
Comptroller of the Currency
3000 Atrium Way, Suite 400B, Mount Laurel, New Jersey 08054

Deputy Associate General Counsel
Board of Governors of the Federal Reserve System
20th & C Streets, N.W., Washington, D.C. 20551

Senior Vice President and General Counsel
Senior Vice President and Lending Officer
Federal Reserve Bank of Philadelphia
10 Independence Mall, Philadelphia, Pennsylvania 19106

After consultation with TD Bank, the Monitor may extend the time period for issuance of the first report for a brief period of time with prior written approval of FinCEN.

Follow-Up Reviews

12. A follow-up, implementation plan review (Second Review) shall commence no later than 90 days after the AML Program Consultant has made its recommendations to TD Bank (unless otherwise agreed by FinCEN). The Monitor shall issue a written second report (Second

Report) within 60 days of commencing the Second Review, setting forth the Monitor's assessment and, if necessary, making recommendations in the same fashion as set forth in Paragraph 11, with respect to TD Bank's plan to execute the Implementation Plan. After consultation with TD Bank, the Monitor may extend the time period for issuance of the Second Report for a brief period of time with prior written approval of FinCEN.

13. Within 60 days after receiving the Monitor's Second Report, TD Bank shall finalize its plan to implement within 180 days all recommendations in the report, unless, within 30 days after receiving the report, TD Bank notifies in writing the Monitor and FinCEN concerning any recommendations that TD Bank considers unduly burdensome, inconsistent with applicable law or regulation, impractical, excessively expensive, or otherwise inadvisable. With respect to any such recommendation, TD Bank need not incorporate that recommendation into the plan to implement all recommendations but shall propose in writing to the Monitor and FinCEN an alternative policy, procedure, or system designed to achieve the same objective or purpose. As to any recommendation on which TD Bank and the Monitor do not agree, such parties shall attempt in good faith to reach an agreement within 30 days after TD Bank serves the written notice.

14. In the event TD Bank and the Monitor are unable to agree on an acceptable alternative proposal, TD Bank shall promptly consult with FinCEN. FinCEN, after consultation with DOJ, OCC, and Federal Reserve as appropriate, may consider the Monitor's recommendation and TD Bank's reasons for not adopting the recommendation in determining whether TD Bank has fully complied with its obligations under the Consent Order. Pending such determination, TD Bank shall not be required to implement any contested recommendation(s).

15. The Monitor shall undertake a follow-up, validation review (Third Review) no later than 60 days after the date by which all SARs have been filed as required by the SAR Lookback

Review. The Monitor shall issue a third report within 180 days of commencing the review, which shall focus on: (i) validating the work that TD Bank undertook to satisfy all recommendations resulting from the AML Program and SAR Lookback Reviews; and (ii) remediating any new issues that the Monitor identifies during the course of the Third Review, including, but not limited to, the required elements of the Consent Order. The recommendations of the Third Report shall follow the same procedures described in Paragraphs 13–14.

16. Following the Third Review, the Monitor shall complete a final, certification review (Fourth Review) to determine whether the Monitor is able to certify that TD Bank's AML program, including its policies and procedures and internal controls, is reasonably designed and implemented to prevent and detect violations of the BSA. The Fourth Review and resulting report, including, if applicable, the accompanying certification, shall be completed and delivered consistent with the requirements set forth in Paragraph 11 no later than 30 days before the end of the Term.

Monitor's Discovery of Potential or Actual Misconduct

17. Except as set forth below in paragraphs (18), (19), and (20), should the Monitor discover during the course of their engagement that any director, officer, employee, agent, third-party vendor, or consultant of TD Bank may have engaged in unlawful activity in violation of the BSA (Potential Misconduct), the Monitor shall immediately report the Potential Misconduct to TD Bank's BSA Officer for further action, unless the Potential Misconduct was already so disclosed. The Monitor also may report Potential Misconduct to FinCEN at any time and shall report Potential Misconduct to FinCEN upon request.

18. In some instances, the Monitor should immediately report Potential Misconduct directly to FinCEN and not to TD Bank. The presence of any of the following factors militates

in favor of reporting Potential Misconduct directly to FinCEN and not to TD Bank, namely, where the Potential Misconduct: (i) poses a risk to public health, safety, or the environment; (ii) involves senior management of TD Bank; (iii) involves obstruction of justice; or (iv) otherwise poses a substantial risk of harm.

19. If the Monitor believes that any Potential Misconduct has occurred or may constitute a criminal or civil violation (Actual Misconduct), the Monitor shall immediately report Actual Misconduct to FinCEN. When the Monitor discovers Actual Misconduct, the Monitor shall disclose the Actual Misconduct directly to FinCEN, and, in such cases, disclosure of the Actual Misconduct to the BSA Officer of TD Bank should occur as FinCEN and the Monitor deem appropriate under the circumstances.

20. The Monitor shall address in their reports the appropriateness of TD Bank's response to disclosed Potential Misconduct or Actual Misconduct, whether previously disclosed to FinCEN or not. Further, if TD Bank or any entity or person working directly or indirectly for or on behalf of TD Bank 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 also immediately disclose that fact to FinCEN and address TD Bank's failure to disclose the necessary information in their reports.

21. Neither TD Bank nor anyone acting on its behalf shall take any action to retaliate against the Monitor for any such disclosures or for any other reason.

Meetings During Term of Monitorship

22. The Monitor shall meet with FinCEN within 30 days after providing each report to FinCEN to discuss the report, to be followed by a meeting between FinCEN, the Monitor, and TD Bank. DOJ, OCC and the Federal Reserve may choose to attend such meetings but will not be

required to do so.

23. At least annually, and more frequently if appropriate, representatives from TD Bank and FinCEN will meet together to discuss the monitorship and any suggestions, comments, or improvements TD Bank may wish to discuss with or propose to FinCEN, including with respect to the scope or costs of the monitorship. DOJ, OCC, and the Federal Reserve may choose to attend such meetings but will not be required to do so.

Contemplated Confidentiality of Monitor's Reports

24. The reports will likely include proprietary, financial, confidential, and competitive business information. Moreover, public disclosure of the reports could discourage cooperation or impede pending or potential government investigations and thus undermine the objectives of the monitorship. For these reasons, among others, the reports and the contents thereof are intended: (i) to be made available to only FinCEN, DOJ, OCC, and Federal Reserve, and (ii) to remain non-public, except as otherwise agreed to by the parties in writing, or except to the extent that FinCEN determines in its exclusive discretion that disclosure would be in furtherance of FinCEN's discharge of duties and responsibilities, or is otherwise required by law.