NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
ONE STATE STREET
NEW YORK, NEW YORK 10004

----------x

In the Matter of :

SKANDINAVISKA ENSKILDA BANKEN AB and, :
SKANDINAVISKA ENSKILDA BANKEN AB, NEW YORK BRANCH

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department"), Skandinaviska Enskilda Banken AB ("SEB"), and the New York Branch of Skandinaviska Enskilda Banken AB (the "New York Branch") (collectively the "Bank") are willing to resolve the matters described herein without further proceedings.

WHEREAS, SEB is a global banking and financial services institution headquartered in Stockholm, Sweden;

WHEREAS, SEB AB is licensed by the Department to operate a foreign bank branch, the New York Branch, in the State of New York;

WHEREAS, SEB AB maintains subsidiaries in the Baltic countries of Estonia, Latvia, and Lithuania: SEB Estonia, SEB Latvia, and SEB Lithuania (collectively, the "Baltic Subsidiaries");

WHEREAS, SEB knew that its Baltic Subsidiaries faced elevated money-laundering risk by processing high-volume transactions for high-risk, non-resident clients;

WHEREAS, SEB had correspondent banking relationships with high-risk banks that were implicated in money laundering;

WHEREAS, in 2019 and 2020, regulators, including the Swedish Financial Supervisory Authority ("S-FSA"), the Estonian Financial Supervisory Authority ("E-FSA"), and the Latvian Financial and Capital Market Commission ("FCMC") flagged deficiencies in SEB's and its Baltic Subsidiaries' Anti-Money Laundering ("AML") controls and transaction monitoring systems, and issued fines as a result;

WHEREAS, the Department investigated various aspects of SEB's historic operations, including whether SEB and its Baltics Subsidiaries' AML program, AML risk containment and diligence measures over their high-risk correspondent banks, and transaction monitoring system violated New York law; and

WHEREAS, the Department finds that, between 2015 and 2019, SEB failed to maintain an effective and compliant AML program in its Baltic Subsidiaries in that it failed to conduct adequate due diligence on non-resident accounts as part of its customer identification program and on its correspondent banking relationships; and that SEB's transaction monitoring system in the Baltic Subsidiaries was inadequate.

NOW THEREFORE, to resolve this matter without further proceedings, pursuant to the Superintendent's authority under Banking Law §§ 39 and 44, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

I. SEB's Operations

1. SEB, a global financial institution headquartered in Stockholm, Sweden, is one of the largest banks in the Nordic region. It has home markets in Finland, Denmark, and Norway. SEB has an extensive presence in the Baltic region as well, operating subsidiaries in Estonia, Latvia, and Lithuania. SEB considers these Baltic countries to be home markets, and these subsidiaries have been designated "Significant Institutions" by the European Central Bank ("ECB").

2. As of June 30, 2026, SEB had total assets worth $479 billion (Swedish krona ("SEK") 4.355 trillion) with assets under management totaling $337 billion (SEK 3.069 trillion).

3. SEB has over 18,000 employees and has a presence in more than 20 locations worldwide, including New York.

4. The Department authorized SEB AB to operate a foreign bank branch in New York (the "New York Branch") in 1987. The New York Branch's operations encompass corporate banking, foreign exchange sales and trading, and treasury operations. During the relevant period, SEB did not clear U.S. dollars through its New York Branch. SEB's New York Branch customers are primarily U.S. subsidiaries of large multinational corporations and mid-sized corporations from SEB's operations in Finland, Denmark, Norway, and Sweden. Some transactions originating in SEB's Baltic Subsidiaries have flowed and continue to flow through the New York Branch.

5. SEB AB established Group-wide compliance control functions, including with respect to AML. Under the SEB Group's internal governance procedures, the Baltic Subsidiaries

and the New York Branch were required to follow the SEB Group's AML compliance controls, established by SEB AB.

II. SEB's Baltic Subsidiaries Operated in a High-Risk Environment

6. Between 2015 and 2019, Estonia, Latvia, and Lithuania were high risk markets; certain customers of the Baltic Subsidiaries had connections to former Soviet Bloc countries and engaged in transactions directed to and from those jurisdictions, which presented an elevated money-laundering risk and required enhanced due diligence and risk management measures.

7. Certain of the Baltic Subsidiaries' domestic clients whose ultimate beneficial owners ("UBOs") were foreign presented potential money laundering risk. As SEB itself noted in its 2019 risk assessments, ex-Soviet Bloc UBOs tended to establish their companies in Lithuania or buy existing ones, which increased the risk of SEB Lithuania being misused by shell companies or businesses engaged in tax avoidance or money laundering schemes.

8. The large numbers of non-resident accounts ("NRAs") presented a heightened money laundering risk for SEB's Baltic Subsidiaries. NRAs were at elevated risk of using the Baltic Subsidiaries for money laundering and tax avoidance schemes.

9. SEB's Baltic Subsidiaries amplified the risk inherent in their high-risk customer base by engaging in high-risk activities, particularly correspondent banking "downstreaming" services, which, as discussed below, did not allow full visibility into the parties to transactions, enabling offshore structures access to SEB's banking systems. At the direction of its U.S. correspondent banks, SEB's Baltic Subsidiaries began to wind down their USD downstreaming in 2015 and completely stopped any USD downstreaming in 2016. SEB, however, continued to engage in downstreaming, on a smaller scale, in other currencies into 2018.

III. SEB's Baltic Subsidiaries Had Deficient AML Controls Between 2015 and 2019

A. The Baltic Subsidiaries' Know Your Customer Control Deficiencies

10. A core component of an effective AML program is an institution's KYC program. A successful KYC program enables financial institutions to establish the identity of a person or entity, assign a risk rating to the customer, and then effectively manage the risk. This first line of defense is critical to combating financial crime. SEB's Baltic Subsidiaries identified deficiencies in their due diligence on NRAs as part of their customer identification program between 2015 and 2019, but repeatedly failed to take measures to enable them to have true insight into their customers' identities.

11. At the time of the conduct described herein, SEB divided its customers into classes based on their AML risk level. SEB's policy was to subject high-risk customers to enhanced due diligence every year; regular-risk customers to regular due diligence every three years; and the lowest risk customers to simplified due diligence every five years. In fact, the Baltic Subsidiaries failed to perform this due diligence as prescribed.

12. Both SEB Latvia and SEB Lithuania delegated their enhanced due diligence reviews to their local branch offices, and in doing so limited the availability of second-level controls. A 2016 internal test of SEB Estonia's KYC data quality for higher risk customers identified deficiencies, including missing tax residency declarations for customers; no information on the main source of funds for customers; missing estimated business volumes for customers—and that the KYC information regarding Politically Exposed Persons ("PEPs") and UBO information was incorrect, misunderstood, or in need of clarification. A 2016 audit report of SEB Lithuania concluded that 3,000 non-active NRAs did not have any relevant KYC information in the files.

13. SEB Estonia's deficiencies were also pronounced as of 2015. SEB Estonia failed to follow its own onboarding processes for private enhanced due diligence clients. By way of example, in an audit of sampled files, 50% of high-risk clients were onboarded without obtaining approval from the Customer Adoption Committee (the "CAC"). After onboarding, SEB Estonia staff changed the risk class designation for some clients without approval from the CAC. And when SEB Estonia did perform due diligence reviews of high-risk private clients, it did not review the customers' activity, even though the bank procedure called for enhanced due diligence given the customers' risk profiles. Additionally, SEB Estonia failed to properly screen the UBOs of its clients: it screened beneficial ownership data against its Financial Sanctions and PEP lists only twice a year, even though it performed these checks monthly for its regular customers. Moreover, in some instances, SEB Estonia's information systems did not contain *any* information about who an ultimate beneficial owner of a client company was. These failures left the Bank at risk of onboarding sanctioned entities.

14. In 2015, SEB internal audits identified a key issue regarding the quality of KYC information throughout the Baltic Subsidiaries. SEB found that the Baltic Subsidiaries failed to update the KYC information of 64% of legal entity clients in their systems. Moreover, 42% of the Baltic Subsidiaries' files that SEB audited did not include customers' beneficial ownership information.

15. Shortcomings in the performance of KYC continued into 2017. At SEB Latvia, 64% of the private person client KYC files did not indicate what country had tax authority over the client based on the client's residency. Moreover, a 2018 sample testing of SEB Latvia's legal person client files revealed missing information, including what services SEB Latvia's clients provided and the countries of residence of clients' main business partners. A 2018 audit report

noted that KYC/AML deficiencies in SEB Estonia's systems also persisted as to private clients, including: missing UBO confirmations, PEP confirmations, employment information, and business relationship information. Additionally, a 2018 sample testing of legal persons customers in SEB Estonia found: (41%) of the legal person files failed to state that the legal person had a connection to Estonia when such a connection existed; (19%) of the files contained no or incomplete UBO information; (13%) of the files were missing PEP declarations; and (10%) of the files did not include any information on the nature of the legal entity's business relationships. SEB Estonia concluded in its 2018 audit report that these gaps in data may lead to incorrect AML risk scoring results or cause PEP and financial sanctions screening activities to be ineffective.

16. In 2018, internal SEB audit reports continued to flag deficiencies in the Baltic Subsidiaries' due diligence and simplified due diligence practices. The Baltic Subsidiaries' due diligence and simplified due diligence practices sometimes relied on information that customers self-reported and did not independently verify information, review customer transactions, and document their due diligence results.

17. The Baltic Subsidiaries' enhanced due diligence remained inadequate as well. Employee adherence to procedure was *ad hoc*. According to a 2018 internal audit report, there were different practices and requirements for documentation of initial enhanced due diligence and of annual enhanced due diligence reviews among the three Baltic Subsidiaries, resulting in varying—and at times poor—qualities of review and different employees coming to different determinations based on similar records, and sometimes without basis in the record.

i. The Baltic Subsidiaries Insufficiently Controlled for Non-Resident Account AML Risk

18. In 2016, the Baltic Subsidiaries failed to effectively manage the risks posed by their high-risk non-resident account ("NRA") customer base. Specifically, the Baltic Subsidiaries' AML procedures contained a conception of risk that was too narrow, focusing on a customer's non-resident status, and not fully capturing other risk factors—such as industry-related AML risks posed by other high-risk clients—that could raise a customer's AML risk profile. SEB's 2016 audits raised the concern that, although the Baltic Subsidiaries had a non-resident customer strategy, it was not formalized as a policy-level document, leading to different approaches across the three Baltic Subsidiaries. The audit identified, as an example, that the strategy did not cover legal entities with non-resident beneficial owners, thus leading to such entities being handled differently across each Baltic Subsidiary. Overall, the audits characterized the Baltic Subsidiaries' high-risk customer strategy as "missing" because the strategy only focused on non-resident customers and not also other high-risk customers.

ii. The Baltic Subsidiaries Implemented a Flawed AML Scoring Model in 2017

19. In 2017, SEB implemented a new AML Risk Scoring model across its three Baltic Subsidiaries. Critically, the model failed to raise a client's AML risk score when the client's file did not include important KYC data. This meant that the Baltic Subsidiaries could improperly rate a high-risk client as a low-risk client and fail to perform the appropriate enhanced due diligence.

20. In addition to relying on this flawed AML risk scoring model, SEB Latvia failed to adhere to its customer risk re-rating procedures, which required that the subsidiary receive approval from SEB's CAC before downrating or uprating any client. Instead, SEB Latvia's own

sample testing in 2018 revealed that it never obtained CAC approval before reducing a customer's risk from one requiring enhanced due diligence to one requiring regular due diligence in the cases analyzed.

iii. SEB's Baltic Subsidiaries Inadequately Performed PEP Screening

21. The Baltic Subsidiaries' audit reports also identified deficiencies in their PEP screenings. SEB Lithuania employees screened PEPs manually and the process for conducting such screenings was not established. Also, a 2018 audit of SEB Latvia found no evidence that the subsidiary performed regular screening of its customer databases against PEP lists. Although SEB Latvia screened customers automatically upon registration in the system and when updating the customer's AML questionnaire, failure to conduct regular PEP screening could expose the Bank to risk if the customer became a PEP after onboarding and diligence but did not notify the Bank. Additionally, SEB Latvia's enhanced due diligence reviews lacked control routines for decisions to terminate enhanced due diligence relationships.

22. A 2018 audit also identified deficiencies in SEB Estonia's PEP screening process. Specifically, the audit observed that SEB Estonia, "performed [PEP screening] manually and no instruction/process [wa]s established for such screening." This deficient approach to PEP screening at SEB Estonia was significant because AML controls regarding PEPs at SEB Estonia were already deficient in other ways: an SEB audit of SEB Estonia identified inaccurate and incomplete collection of KYC information for PEPs as a key concern. SEB Estonia's flawed PEP screening coupled with inaccurate PEP KYC measures presented a breakdown in compliance.

IV. SEB's Baltic Subsidiaries Exposed Financial Institutions in New York, Specifically, and the U.S. Financial System, Generally, to Elevated Financial Crimes Risk

23. Between 2006 and 2019, approximately $300 million worth of transactions originating from the Baltic Subsidiaries passed through the New York Branch; $2.5 million of

which occurred between 2015 and 2019. Additionally, U.S. financial institutions—including banks located in New York and licensed by the Department, such as USD Clearing Bank 1—were exposed to the financial crimes risk from SEB and its Baltic Subsidiaries through SEB's use of their U.S. dollar clearing services.

24. Between 2015 and 2019, USD Clearing Bank 1 processed $144 billion worth of transactions with SEB's Baltic Subsidiaries. USD Clearing Bank 1 processed these transactions notwithstanding its own concerns about doing business with SEB. Specifically, in 2016 USD Clearing Bank 1 expressed concern about the number of money service businesses ("MSBs") and other high-risk industries in the Baltics; the large number of non-resident customers banking in the Baltics; Estonia and Latvia being inherently high money-laundering risk countries; that SEB's transaction patterns were similar to those of a well-known European bank implicated in a major money-laundering scandal; and that SEB was enabling transactions involving PEPs who were UBOs of SEB clients without conducting appropriate screening.

25. In response to this risk, a leader in SEB's Financial Institutions Unit, based in Lithuania, wrote: "What we need to do [is]…review our whole non-resident client base (currently only 1000 clients are in the non-resident client department - the rest of 11,000 are scattered within the bank without any specific strategy or annual review of transactions)."

26. In response, the employee's manager at the Baltic Division asked for an update on what steps the Bank had taken to analyze non-residential accounts in the Baltics and what the Bank should do in the future to manage its non-resident clients. At the time, each of the Baltic Subsidiaries was in the process of establishing strategies to address the non-resident issue, but had not finalized or implemented new strategies, leaving the Baltic Subsidiaries unable to effectively manage the risks of their non-resident clients.

27. SEB and its Baltic Subsidiaries also used another U.S. financial institution, USD Clearing Bank 2, to clear USD. Between 2017 and 2019, USD Clearing Bank 2 cleared $131 billion worth of transactions involving SEB's Baltic Subsidiaries.

28. The elevated money laundering risks in SEB's Baltic Subsidiaries were thus imported into the U.S. financial system and specifically to New York, through SEB's New York Branch and SEB's Baltic Subsidiaries' USD clearing relationships with New York-based institutions.

V. Billions of Dollars in High-Risk Correspondent Bank Transactions with Foreign Financial Institutions Flowed Through SEB

29. SEB's relationships with foreign financial institutions exposed it to some of Europe's largest money laundering scandals. Between 2015 and 2019, SEB engaged in transactions with multiple high-risk foreign financial institutions, including: a large European bank and its Baltic Branch ("European Bank 1" and "European Bank 1 – Baltic Branch," respectively) that were implicated in a money laundering scandal involving hundreds of billions of dollars' worth of suspicious transactions; another bank previously designated as a "primary money laundering concern" by the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") ("European Bank 2"); another bank implicated in significant money laundering activity ("European Bank 3"); a bank later placed into liquidation for AML violations ("European Bank 4");[1] and a major financial institution sanctioned for systemic AML failures ("European Bank 5").

[1] In 2014, the Organized Crime and Corruption Reporting Project ("OCCRP") reported that European Bank 3 and European Bank 4 were two of a number of banks that laundered $20 billion from Russian shell companies into banks throughout the European Union and beyond between 2010 and 2014, commonly known as the Russian Laundromat. In 2019, the OCCRP reported that the Russian Investment Bank Troika Dialog laundered approximately $5 billion out of Russia into Europe between 2003 and 2013, some of which was laundered through European Bank 4 and European Bank 3, commonly known as the Troika Laundromat.

A. SEB Employed Deficient Correspondent Bank AML Controls

30. SEB's diligence review of its correspondent bank partners was deficient. SEB performed only simplified due diligence—the lowest form of diligence—on several of its high-risk correspondent banking partners. Moreover, SEB's customer files on these correspondent banks were deficient, SEB calculated correspondent bank AML risk incorrectly, and SEB failed to update the KYC procedures governing correspondent bank relationships and were thus out of compliance.

31. SEB's provision of high-risk "downstreaming" services—including in USD transactions—through its correspondent banking relationships also increased its money-laundering risk. A correspondent banking relationship occurs when a foreign institution, the correspondent bank, establishes accounts at and sends payments through a respondent bank, here, SEB, thereby allowing the foreign institution to offer global banking services without establishing physical branches abroad. Downstreaming occurs when a respondent bank enables transactions for other banks outside of the correspondent banking relationship without full transparency into the originating bank, heightening the AML risk picture.

32. A 2019 SEB internal analysis revealed that, between 2008 and 2017, correspondent banks made hundreds of millions of dollars-worth of downstreaming payments through the Baltic Subsidiaries to offshore companies.

B. SEB Failed to Adequately Vet Its Correspondent Banking Relationships with European Bank 1 and European Bank 1 - Baltic Branch

33. Between 2015 and 2019, SEB provided correspondent banking services to European Bank 1, holding accounts for it in USD and several other currencies. In addition to its

correspondent banking services, SEB and European Bank 1 were counterparties in a number of other financial products and services.

34. SEB characterized European Bank 1 as "an important counterpart bank in SEB's home-market" with whom SEB shared "significant" trading activity. The volume of transactions bears this out: between 2008 and 2018, SEB processed approximately $5.17 trillion through correspondent banking accounts that SEB maintained on behalf of European Bank 1; $600 billion of which occurred between 2015 and 2018. These transactions all occurred in SEK. In addition, between 2008 and 2018, SEB's New York Branch engaged in 669 transactions worth more than $300 million to or from European Bank 1; $120 million of which occurred between 2015 and 2018. These transactions were enabled through a Society of Worldwide Interbank Financial Telecommunication ("SWIFT") Relationship Management Application ("RMA") key shared by the New York Branch and European Bank 1's head office. RMA is a filter mandated by SWIFT which allows financial institutions to decide which counterparties are able to send financial information messages. This gives financial institutions the ability to block unwanted messages and allow others.

35. SEB's Baltics Subsidiaries also worked with European Bank 1's – Baltic Branch. For example, SEB Estonia and European Bank 1 – Baltic Branch partnered in a number of financial products and services. SEB Estonia held a Euro account for European Bank 1 – Baltic Branch from December 2011 to May 2017. Separately, SEB Latvia and SEB Lithuania maintained RMA keys with European Bank 1 – Baltic Branch.

36. In 2012, a European financial regulator published a report about European Bank 1's activities. By March 2017, journalists were sounding the alarm about suspicious transactions flowing through European Bank 1 – Baltic Branch. Notwithstanding this information, SEB

continued to perform its lowest level of diligence on European Bank 1. SEB Estonia began to perform enhanced due diligence on European Bank-1 – Baltic Branch in 2016, and terminated that correspondent relationship in 2017.

37. In SEB's May 2018 AML/KYC Review, SEB employees identified risks related to European Bank 1. The review noted the allegations that European Bank 1 – Baltic Branch was used for money laundering between 2007 and 2015. The review also referenced a criminal investigation into European Bank 1, noting that the law enforcement agency wanted to know how hundreds of billions of dollars from Russia and other former Soviet states entered Europe through a branch of European Bank 1. The review found that European Bank 1 acknowledged that its controls were "manifestly insufficient" and that its governance was deficient.

38. Notwithstanding these conclusions, SEB continued its relationship with European Bank 1 and European Bank 1 – Baltic Branch; it was only in October 2018 that SEB's CAC imposed an enhanced due diligence requirement on European Bank 1. SEB memorialized this decision in an internal AML/KYC diligence form that highlighted the criminal investigation, finding that European Bank 1 acknowledged that European Bank 1 – Baltic Branch's procedures, "had been . . . inadequate, including, *inter alia*, lack of identification of 'controlling interests' of customers, lack of screening of customers, and lack of independence and possible internal collusion in the [European Bank 1 – Baltic Branch]."

39. Later that year, in response to continued adverse media reports about European Bank 1 – Baltic Branch and the major European Bank 1 money laundering scandal, SEB terminated its remaining relationships with European Bank 1 – Baltic Branch. Between 2008 and 2018, SEB engaged in more than $7 billion worth of European Bank 1 – Baltic Branch transactions; $233 million of which occurred in USD between 2015 and 2018.

C. SEB's AML/KYC Reviews of European Bank 5 Were Deficient

40. European Bank 5 was one of the largest private banks in the Baltic region. In 2016, European Bank 5's local regulator levied an administrative fine against European Bank 5 to address assorted AML failings, including failing to appropriately monitor unusual transactions. In 2018, a U.S. regulator named European Bank 5 an institution of primary money laundering concern and noted that European Bank 5's management permits the bank and its employees to engage in money laundering schemes. As discussed below, SEB did not appropriately mitigate the risk posed by its relationship with European Bank 5.

41. Between 2008 and 2018, SEB engaged in more than $12 billion worth of transactions with European Bank 5; $1.8 billion of which occurred in USD between 2015 and 2018. This relationship encompassed the exchange of SWIFT RMA keys, correspondent banking services (through SEB's provision of accounts to European Bank 5), in addition to other services. Further, SEB held accounts for European Bank 5 in several currencies primarily for payments incidental to custody services. These accounts were also used on occasion for commercial payments to SEB customers.

42. In 2016, SEB's AML/KYC Review of European Bank 5 noted that European Bank 5 was fined by its local regulator for KYC failures relating to its high-risk clients. While SEB Latvia performed enhanced due diligence on European Bank 5, SEB only employed simplified due diligence on the bank and did not perform any site visits to assess the risk of working with European Bank 5.

43. Moreover, the AML/KYC Review forms that SEB used for European Bank 5 at that time were devoid of much information, a departure from SEB's own practice for other partner banks and below industry standard. SEB should have assessed, among other relevant

information, country-specific risks, the risks of the products European Bank 5 used, the client-base risk, and risks of the industries in which the bank participated. SEB's AML/KYC Review form did not include this information, however. Some of the information existed elsewhere within SEB, but SEB did not integrate the information into its main AML/KYC assessment. For example, SEB noted in other diligence forms that RMA and Loro Account services were "high risk" products. But this finding was not reflected in SEB's AML/KYC forms on European Bank 5, which remained virtually unchanged year-to-year, reflecting a review process that was static and failed to evolve with European Bank 5's increasing AML risk picture.

44. SEB's inadequate risk analysis persisted until 2018, at which time SEB finally terminated its relationship with European Bank 5 after a U.S. regulator found that European Bank 5's management permitted the bank and its employees to engage in money laundering schemes, and that high-risk shell company activity enabled the bank and its customers to launder funds. That U.S. regulator also found that European Bank 5 maintained inadequate controls over high-risk shell company accounts and sought to obstruct enforcement of AML rules.

D. *SEB's Downstreaming Practices Compounded the Risks in its Correspondent Bank Relationships*

45. As a 2019 internal SEB email noted: "Correspondent banks (including SEB) have been and are worried about the downstreaming as this is a high(er) risk practice and this is of [sic] even more risky combined with high-risk countries."

46. The internal investigation conducted by SEB following the European Bank 1 money laundering scandal revealed that downstreaming was enabling transactions initiated by offshore companies at SEB Lithuania. The investigation also made clear that U.S. financial institutions were exposed to SEB's downstreaming.

47. In SEB Estonia, the review looked at 3.36 billion EUR worth of downstreaming occurring between 2008 and 2018 and found that downstreaming included USD transactions, and transactions originating from European Bank 4. The review observed that a notable number of fund transfers from Russia into the EU occurred through SEB Estonia's downstreaming. The review also found matches against SEB's internal "sensitive names list,"[2] representing 7 million EUR worth of transactions in SEB Estonia that were also connected to money laundering scandals.

48. In SEB Lithuania, the review observed that four banks, including European Bank 5, discussed above, comprised 1.1 billion EUR of downstreaming flows between 2008 and 2017 involving SEB Lithuania. The downstreaming included USD transactions and other transactions where the ultimate destination was U.S. financial institutions, including SEB's clearing partner, USD Clearing Bank 1. Distilling this data further, SEB assessed that the top 10 initiators and beneficiaries of these transaction flows accounted for transactions totaling 574 million EUR. Of this, 525 million EUR were connected to offshore companies. In addition, 10 transactions included parties that matched the SEB "sensitive names list." In sum, the analysis concluded that a "notable portion" of these downstreaming flows were "linked to counterparties that are offshore companies" with scant links to local Lithuanian business activity.

49. SEB's downstreaming exacerbated the financial crimes risk that came with banking with its troubled correspondent banks. Despite being on notice of the high risks involved in the practice, SEB continued downstreaming until its U.S. correspondent banks directed it to wind down the practice in 2015; however, SEB continued downstreaming, on a smaller scale, into 2018 in other currencies. SEB completely stopped any USD downstreaming in 2016.

[2] SEB's sensitive names list was a list of more than 2,000 names that SEB compiled, drawing from various sources reporting on relevant money laundering stories.

VI. SEB's Baltic Subsidiaries' Transaction Monitoring Deficiencies

50. SEB's Baltic Subsidiaries used SEB's transaction monitoring system, known as Financial Crime Risk Management ("FCRM"). As is typical with transaction monitoring systems, FCRM was configured with predefined scenarios designed to simulate methods of money laundering and suspicious activity. The FCRM system processed preceding day transactional data and flagged transactions with suspicious and unusual patterns that matched those scenarios.

51. FCRM failed to effectively identify suspicious transactions. A 2018 internal audit identified that, in the first instance, SEB's Baltic Subsidiaries did not ensure proper controls on data deliveries into FCRM to function properly, reducing the effectiveness of FCRM. Another 2018 internal audit also noted weaknesses regarding scenario definitions designed to replicate known methods of money laundering. SEB's Baltic Subsidiaries were aware of this problem, but did not resolve it promptly.

52. SEB's Baltic Subsidiaries' response to FCRM alerts indicating possible money laundering or suspicious activity was also deficient. Quality control is critical to ensuring that institutions investigate alerts in a timely and consistent manner. According to a 2018 internal audit of SEB Estonia, in particular, poor FCRM alert processing resulted in two key failings: First, FCRM "PEP alerts" were based on an incorrect scenario matrix and SEB Estonia failed to investigate them consistently, thereby missing potential matches relevant to risk rating, and instead simply closed alerts as they came in—sometimes up to 100 per day. Second, when SEB Estonia closed out alerts, it often relied on outdated standardized forms, not tailored to each unique case, and in doing so sometimes inaccurately noted that it had investigated an alert when, in fact, it had not.

53. Additionally, a 2018 SEB audit revealed that SEB's FCRM alert processing was backlogged significantly at all three Baltic Subsidiaries. For a period in 2017, it seemed that SEB's Baltic Subsidiaries had resolved this issue, but the problem returned later that year, leading to backlogs at all three Baltic subsidiaries. As of January 2018, SEB Latvia and SEB Lithuania had resolved their backlogs, but SEB Estonia had still not resolved its own.

54. At times, the FCRM system failed to generate alerts. SEB Estonia's AML Compliance team discovered that, between July 6, 2017, and August 10, 2017, the "FCRM system did not create any new alerts for Estonia." The AML Compliance team deduced that this lack of FCRM alerts generation occurred because the process to initialize alert generation in the FCRM system was started but never completed. Without alerts generation for over one month in FCRM, SEB Estonia's transaction monitoring apparatus was—by definition—deficient. SEB subsequently ran manual monitoring and analyzed the transactions received during this time period.

55. SEB also employed the SafeWatch system to screen transactions. Unlike FCRM, which focused on retrospective monitoring for certain money laundering scenarios, SafeWatch was designed to work in real time, flagging transactions that involved sanctioned individuals or entities, blacklisted entities, or PEPs.

56. Like FCRM, SafeWatch was beset by issues. SafeWatch provided staff with three options for handling alerts: release, assign to the compliance team, or block. SEB's 2018 audit noted that SafeWatch did not document the justification for these decisions, however, nor did SEB do so outside of the system. SEB also failed to perform regular and documented quality assurance to ensure that Baltic Subsidiary staff was properly processing alerts.

57. SEB's Baltic Subsidiary staff failed to screen all customers and transactions against sanctions lists in SafeWatch, leaving open the possibility that the Baltic Subsidiaries were facilitating transactions to or from sanctioned individuals or entities.

58. SEB also did not have a backup system in place to allow for compliant processing if SafeWatch became unavailable. A 2018 audit report noted that payments were processed without screening when SafeWatch was not available in SEB Estonia and SEB Latvia. In 2018, SEB's auditors observed that, "[w]hen SafeWatch system is not available, payments are processed without screening against sanction lists." SEB manually reviewed the transactions afterwards for the transactions processed when SafeWatch was down. In addition to OFAC and EU sanctions lists, SEB maintained SafeWatch's voluntary internal lists of restricted countries, correspondent bank restrictions, and fraud-connected parties, but did not regularly review these internal lists and remove old information leading to inefficiencies and false matches.

59. Even when the FCRM and SafeWatch systems detected suspicious transactions, SEB's Baltic Subsidiaries' escalation of alerts for further investigation—such as the performance of legally-mandated investigatory steps including the filing of suspicious activity reports ("SARs")—was not sufficiently robust. Consequently, SEB's Baltic Subsidiaries failed to submit SARs or delayed submitting SARs it should have submitted and failed to properly investigate suspicious transactions. A 2018 audit identified some instances where SEB Latvia failed to submit SARs for over a month. In other instances, KYC staff at SEB Latvia failed to relay transaction information to SEB's Compliance Department for assessment of whether SEB should file a SAR. SEB auditors concluded, after review of sampled files, that they had no way of knowing whether SEB Latvia made timely SAR submissions—or reported at all when it should have. They further concluded that in SEB Lithuania it was not possible to reconcile suspicious

activity reporting to verify its completeness and timeliness because the reports were stored in different sources.

60. Finally, each of the three Baltic Subsidiaries designated a single employee to submit SARs and perform related investigations, forgoing the basic and prudent practice of quality control checks.

61. SEB and its Baltic Subsidiaries were well aware of these failings. Indeed, SEB acknowledged fault in its 2008-2015 SAR filing practices for its highest risk customers in its 2018 Annual Group Internal Audit Report. It did so again in 2019 in a presentation to the S-FSA.

Cooperation and Remediation

62. The Department has given weight to SEB's cooperation with the Department throughout this investigation, including its timely and appropriate responses to requests for information. Additionally, the Department recognizes SEB's remediation of the deficiencies identified in this Consent Order.

Violations of Law and Regulations

63. SEB failed to maintain an effective and compliant anti-money laundering program, in that it failed to conduct adequate due diligence on non-resident accounts as part of its customer identification program, as well as on its correspondent bank and RMA relationships, in violation of 3 N.Y.C.R.R. § 116.2.

64. SEB failed to maintain an adequate transaction monitoring system in violation of 3 N.Y.C.R.R. § 504.3.

NOW THEREFORE, to resolve this matter without further proceedings, the Department and SEB stipulate and agree to the following terms and conditions:

SETTLEMENT PROVISIONS

Monetary Provisions

65. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order the Bank shall pay a total civil monetary penalty pursuant to New York Banking Law §§ 39 and 44 to the Department in the amount of thirty-three million U.S. dollars ($33,000,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

66. The Bank shall not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

67. The Bank shall neither seek nor accept, directly or indirectly, reimbursement or indemnification with respect to payment of the penalty amount, including but not limited to, payment made pursuant to any insurance policy.

Full and Complete Cooperation of the Bank

68. Consistent with applicable law, the Bank commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order.

Breach of Consent Order

69. In the event that the Department believes any party to this Consent Order to be in material breach of the Consent Order, the Department will provide written notice to the party, and the party must, within ten (10) business days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate

that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

70. The parties understand and agree that the party's failure to make the required showing within the designated time period shall be presumptive evidence of the party's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all the remedies available to it under New York Banking and Financial Services Law and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Waiver of Rights

71. The parties understand and agree that no provision of this Consent Order is subject to review in any court or tribunal outside the Department.

Parties Bound by the Consent Order

72. This Consent Order is binding on the Department and the Bank as well as any successors and assigns that are under the Department's supervisory authority. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

73. No further action will be taken by the Department against the Bank for the conduct set forth in the Consent Order, provided that the Bank comply with the terms of the Consent Order.

74. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against the Bank for transactions or conduct that was not disclosed in the written materials submitted to the Department in connection with this matter.

Notices

75. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Avery Heisler
Enforcement Counsel for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

Christina Glekas
Enforcement Counsel for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

Joseph C. Mineo
Enforcement Counsel for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One Commerce Plaza
Albany, NY 12210

Ching-Huei Li
Enforcement Counsel for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For SEB

Hans Ragnhäll
General Counsel
SKANDINAVISKA ENSKILDA BANKEN AB (PUBL)
Kungstradgardsgatan 8, SE-106 40, Stockholm, Sweden

John Arne Wang
General Manager, SEB New York Branch
SEB AB NEW YORK BRANCH
66 Hudson Boulevard, New York, New York 10001

David Esseks
Esseks Ingoglia
350 Fifth Avenue, The Empire State Building, Suite 5310
New York, NY 10118
Counsel to SEB

Anthony Mansfield
Allen Overy Shearman Sterling US LLP
1101 New York Avenue, NW
Washington, DC 20005
Counsel to SEB

Miscellaneous

76. This Consent Order and any dispute thereunder shall be governed by the laws of the State of New York without regard to any conflicts of laws principles.

77. This Consent Order may not be altered, modified, or changed unless in writing and signed by the parties hereto.

78. This Consent Order constitutes the entire agreement between the Department and the Bank and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order.

79. Each provision of this Consent Order shall remain effective and enforceable against the Bank, its successors, and assigns, until stayed, modified, suspended, or terminated by the Department.

80. In the event that one or more provisions contained in this Consent Order shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

81. No promise, assurance, representation, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of the Consent Order.

82. Nothing in this Consent Order shall be construed to prevent any consumer or any other third party from pursuing any right or remedy at law.

83. This Consent Order may be executed in one or more counterparts and shall become effective when such counterparts have been signed by each of the parties hereto (the "Effective Date").

[*remainder of page intentionally left blank*]

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s/ Elizabeth A. Farid
ELIZABETH A. FARID
Senior Enforcement Counsel
Consumer Protection and Financial Enforcement

October 15, 2026

By: /s/ Kathryn A. Taylor
KATHRYN A. TAYLOR
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement

October 15, 2026

By: /s/ Christopher B. Mulvihill
CHRISTOPHER B. MULVIHILL
Deputy Superintendent Consumer Protection and Financial Enforcement

October 15, 2026

By: /s/ R. Gabriel D. O'Malley
R. GABRIEL D. O'MALLEY
Executive Deputy Superintendent Consumer Protection and Financial Enforcement

October 15, 2026

SKANDINAVISKA ENSKILDA BANKEN AB (publ)

By: /s/ Cecilia Wolrath Ekenbäck
CECILIA WOLRATH EKENBÄCK
Head of Group Compliance

October 14, 2026

By: /s/ Hans Ragnhäll
HANS RAGNHÄLL
General Counsel

October 14, 2026

SEB NEW YORK BRANCH

By: /s/ John Arne Wang
JOHN ARNE WANG
General Manager, SEB New York Branch

October 14, 2026

ESSEKS INGOGLIA

By: /s/ David Esseks
DAVID ESSEKS
Counsel to SEB

October 14, 2026

ALLEN OVERY SHEARMAN STERLING US LLP

By: /s/ Anthony Mansfield
ANTHONY MANSFIELD
Counsel to SEB

October 14, 2026

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Kaitlin Asrow_____
KAITLIN ASROW
Acting Superintendent of Financial Services

October 14, 2026