

C L I F F O R D
C H A N C E

REPORT OF INVESTIGATION ON SWEDBANK AB (publ)
EXECUTIVE SUMMARY

23 MARCH 2020

CLIFFORD CHANCE US LLP

**2001 K STREET NW
WASHINGTON, DC 20006-1001
TEL +1 202 912 5000
FAX +1 202 912 6000**

**31 WEST 52ND STREET
NEW YORK, NY 10019-6131
TEL +1 212 878 8000
FAX +1 212 878 8375**

EXECUTIVE SUMMARY

Clifford Chance designed the Investigation to identify historical deficiencies in Swedbank's AML compliance systems and controls from January 2007 through March 2019 (the "Investigation Period"). The Investigation focused on the areas of Swedbank and the Baltic Subsidiaries that, based on the available information, evinced the highest historical AML-related risk. In this regard, the scope and focus of the Investigation was informed by the media allegations regarding Swedbank, the pending investigations by Swedish, Baltic and US authorities, Swedbank's own prior internal reviews that had identified historical issues, and, on an iterative basis, information identified through Clifford Chance's analysis of internal documents and communications, customer and transaction records, and interviews of current and former employees at every level of the institution and across each of its four home markets.

Methodology

The Investigation was broad and intensive, and considered billions of transaction records, approximately 160 million customer records, over 38 terabytes of electronic and scanned hard copy data from Swedbank's internal files, including over 20 million documents gathered from email servers, employee laptops and mobile devices, shared server files, KYC materials, internal audit reports, and Board and key committee minutes and supporting materials. This data was reviewed against targeted search terms, which were adjusted as we learned more as the Investigation progressed. The Investigation involved the collection and review of relevant documents in multiple languages, including Swedish, Estonian, Latvian, Lithuanian and Russian.

Clifford Chance conducted nearly 100 interviews of 81 individuals, including current and former employees, managers and senior executives, current and former Board members, and an external counsel. Throughout the Investigation, Swedbank took steps to retain all potentially relevant data and documents and facilitated Clifford Chance's unfettered access to documents, data and personnel.

In addition, steps were taken, on the advice of local counsel, to ensure compliance with applicable privacy, bank secrecy, employment and other relevant legal regimes. While the manner in which certain facts and findings are discussed in this Report has been impacted by applicable Swedish, Estonian, Latvian and Lithuanian privacy and bank secrecy laws and regulations, in our view, the Report provides a clear picture of what happened, how it happened, and the accountability of those involved.

AML Controls

Over the course of the Investigation Period, AML regulations have evolved, as have their interpretation and application by international banks operating in Europe. Industry standards have also evolved, based on common practices, official guidance and past enforcement actions, with regulatory expectations increasing over time. It is important to understand the facts discussed herein against this backdrop rather than solely through today's lens and with the benefit of hindsight.

As is set forth in detail in this Report, based on the available information, Clifford Chance did not conclude that Swedbank engaged in money laundering or processed customer transactions that constituted the proceeds of crime. Among other things, this would require definitive knowledge of a customer's source of funds, which was not available. However, the Investigation did reveal that Swedbank, throughout the Investigation Period and to varying degrees across LC&I, Swedish Banking and Baltic Banking, had inadequate systems and controls to ensure proper management of the AML and economic sanctions risk of its customer base, which, therefore, historically exposed Swedbank and the Baltic Subsidiaries to significant AML and sanctions risk.

This risk appeared most prevalent in the Baltic Subsidiaries, primarily at Swedbank Estonia, and principally arose from the high risk non-resident ("HRNR") business.

From before 2007 until a decision to de-risk the HRNR business in 2016, Swedbank Estonia and Swedbank Latvia actively pursued these high risk customers as a business strategy. Swedbank Estonia also accepted certain customers that had been off-boarded by another bank in Estonia in 2015 that had decided to exit the HRNR business based on excessive money laundering risk.

Although Swedbank Estonia created a special committee to review the on-boarding and maintenance of HRNR customers, the Investigation has identified that this committee approved high risk customers without having complete documentation regarding the ultimate beneficial owners (“**UBOs**”), proof of source of funds or explanation of the legitimate business purpose of the customers, and did not address red flags that arose from the information that was provided. Some of the companies had complex and opaque ownership structures involving off-shore entities organized in low tax jurisdictions, as well as ownership through foreign trusts and similar vehicles for which the UBOs were difficult to verify. Swedbank Estonia also accepted customers despite awareness amongst employees, including relationship managers (“**RMs**”), that the listed beneficial owners were not the actual UBOs, and in situations in which the prospective customer refused to provide verifiable beneficial ownership information.

In addition, at Swedbank Estonia, employees involved in the HRNR business kept certain information regarding the UBOs for some customers outside of Swedbank’s regular customer databases and retained the information in hard copy in a safe or locked drawer to assuage the customer’s concern that the true UBOs may become known to third parties. Swedbank Estonia employees also accepted customer corporate structures knowing that they were designed to conceal the true UBOs from home country tax authorities. Lastly, Swedbank Estonia employees also repeatedly overlooked or disregarded indications of potentially suspicious transactions. Some of these practices were also identified in the other Baltic Subsidiaries. The AML deficiencies were not limited to the Baltic Subsidiaries, as certain of the high risk customers that banked primarily in the Baltics also were permitted to open and to maintain accounts with Swedbank LC&I and Swedish Banking.

AML Forensic Analysis

The Investigation analyzed forensically the external payment transactional activity of Baltic Banking customers that met the Baltic Subsidiaries’ definition of HRNR customer, namely customers that were non-resident legal entities registered outside of the EU and Norway but also including customers registered in Malta, Cyprus, the UK or Luxembourg, which customers Swedbank had rated as high risk at some point during the Investigation Period. This definition, as applied to the full customer base of the Baltic Subsidiaries, could include entities that today would not be considered to have high AML risk, but could exclude other customers who did present high AML risk. To avoid excluding such customers from the review, the Investigation also considered additional categories of customers, such as (a) customers identified in the course of the Investigation as presenting AML risk, (b) customers that had done business through Swedbank with counterparties at certain high risk Baltic banks identified by government authorities or in the media as being involved in money laundering schemes and (c) customers with strong links to certain foreign jurisdictions, either through residency or ownership.

FTI collected transaction data for this aggregate group of customers (“**AML Risk Identified Customers**”) for the period from March 2014 through March 2019, and ran 21 algorithmic detection scenarios designed to identify potentially suspicious transactions. Inclusion in the group of AML Risk Identified Customers is not necessarily indicative of suspicious behavior or improper conduct. Rather, these parameters were designed to capture the portion of the Baltic Subsidiaries’ customer population that warranted further review. In addition, the fact that an external payment to or from one of these customers hit against one or more of the detection algorithms does not mean that the payment should have been considered suspicious at the time, let alone is it

evidence that a customer engaged in money laundering or other financial crime. Rather the detection algorithms are designed to identify transactions with risk indicators similar to those that a transaction monitoring system would flag for further review. To provide further context, industry wide, typically less than 10% of hits against detection algorithms result in a report of a suspicious transaction to an appropriate financial intelligence unit (“**FIU**”). In other words, the false positive rate often exceeds 90%.

In presenting the results of this analysis, Clifford Chance has focused on external transactions that alerted on three or more detection scenarios.

For Swedbank Estonia, during the five-year period from March 2014 through March 2019, this exercise identified payments that totaled approximately €9.9 billion that were received into these customers’ accounts, and a total of approximately €11.4 billion that were sent by these customers from their accounts.

For Swedbank Latvia, during the five-year period from March 2014 through March 2019, this exercise identified payments that totaled approximately €4.8 billion that were received into these customers’ accounts, and a total of approximately €4.5 billion that were sent by these customers from their accounts.

For Swedbank Lithuania, during the five-year period from March 2014 through March 2019, this exercise identified payments that totaled approximately €3.2 billion that were received into these customers’ accounts and a total of approximately €3.0 billion that were sent by these customers from their accounts.

Thus, across all three Baltic Subsidiaries the total value of external payments that alerted on three or more detection scenarios during the five-year period from March 2014 through March 2019 was approximately €17.8 billion of incoming and €18.9 billion of outgoing payments.

Significantly, the value of transactions meeting these criteria decreased materially on an annual basis over the period from 2014 through 2019 for Swedbank Estonia and Swedbank Latvia. For example, at Swedbank Estonia, incoming payments decreased from a high mark of approximately 9.5% of the total incoming payments of all customers for Swedbank Estonia over the last three quarters of 2014, to approximately 1.1% of the total incoming payments in Q1 2019. Similarly, at Swedbank Latvia, incoming payments decreased from a high mark of 6.8% of the total incoming payments of all customers for Swedbank Latvia in 2015, to 0.9% of the total incoming payments in Q1 2019. At Swedbank Lithuania, the overall relevant transaction activity was lower than at Swedbank Estonia and Swedbank Latvia, but increased to a high of approximately 2.8% of the total incoming payments for all customers of Swedbank Lithuania in 2018.

US Sanctions Forensic Analysis

The Investigation also included an assessment of potential non-compliance by the Baltic Subsidiaries or their customers with the sanctions regulations of the US Treasury Department’s Office of Foreign Assets Control (“**OFAC**”). In particular, based on data collected and processed by FTI, Clifford Chance reviewed USD Society for Worldwide Interbank Financial Telecommunications (“**SWIFT**”) network payments processed by the Baltic Subsidiaries during the five-year period from March 22, 2014 through March 22, 2019 to identify whether any such payments may not have complied with OFAC blocking sanctions or country embargos, which we then characterized as “**Subject Transactions.**” As part of this process, Clifford Chance also reviewed available customer data to identify any OFAC-sanctioned customers of the Baltic Subsidiaries and to ensure the inclusion of their USD SWIFT payments in the OFAC transaction review.

For the five-year period under review, covering approximately 26.6 million transaction messages and 1.8 million USD payments, Clifford Chance identified 582 Subject Transactions, totaling approximately \$4.76 million, processed by the Baltic Subsidiaries.

Within this total, by Baltic Subsidiary, Clifford Chance determined that:

- Swedbank Estonia customers used an online banking platform to initiate 19 outgoing Subject Transactions, totaling approximately \$100,000, which appeared to involve persons in Iran, Cuba or Crimea. We also identified 35 apparent incoming Iran-related Subject Transactions, totalling approximately \$222,000.
- Swedbank Latvia customers used an online banking platform to initiate 522 outgoing Subject Transactions, totaling approximately \$4.43 million, of which 507 such outgoing Subject Transactions between 30 December 2014 and 30 December 2016, amounting to approximately \$4.26 million, involved three shipping customers domiciled in offshore jurisdictions that had accounts at Swedbank Latvia but whose owner appeared to operate these companies from Crimea. The remaining 15 outgoing Subject Transactions from accounts at Swedbank Latvia appeared to involve non-sanctioned customers who were temporarily located in Crimea or Iran or payments by non-sanctioned customers to counterparties in Crimea. We also identified one incoming Subject Transaction for \$5,970 to an individual customer of Swedbank Latvia who had a residency address in Crimea.
- Swedbank Lithuania customers used an online banking platform to initiate five outgoing Subject Transactions, totaling approximately \$2,400 that appeared to involve persons in Crimea.

None of these Subject Transactions involved any OFAC-listed persons, and nearly all of them, by volume and value, occurred prior to 2017, the year that the Baltic Subsidiaries implemented an automated payment screening solution.

Governance

Since 2016, Swedbank initiated enhancements to its compliance control and risk management systems in the Baltic Subsidiaries. However, these efforts were impeded by a number of governance failings. For example, Swedbank senior management historically had failed to establish clear lines of AML-related responsibilities, particularly as between the business (the first line of defense) and Compliance (the second line of defense), or to ensure methods of challenge by the second line over the AML-related functions appointed to the first line of defense. In addition, throughout the Investigation Period, the Swedbank CEOs appeared to lack an adequate appreciation for the severe risk posed to the institution by the HRNR business in Baltic Banking, given the consistently ineffective AML controls. This lack of appreciation for the degree of risk was evidenced by the Bank's failure to adopt a Group-level AML risk appetite statement until 2017, or to take steps to ensure consistency of approach to risk rating customers across business lines.

The Investigation also found that because senior management failed to appreciate the degree of legal and reputational risk to Swedbank, it did not always engage with the Board in a manner consistent with the importance of these issues. For example, throughout the Investigation Period GIA repeatedly identified and reported serious AML control deficiencies which were raised to the Audit Committee of the Board and often summarized to the full Board, particularly during the period from 2016 through early 2019. The messaging on balance by the CEO and other senior executives to the Board during this period was that while there were problems, they were under control. Similarly, during this period, the Group Compliance function internally and with the assistance of outside experts such as the law firm Erling Grimstad AS ("**Grimstad AS**"), had identified serious AML control deficiencies and potentially serious legal risk to Swedbank arising from those deficiencies. In some cases, the more serious findings were not escalated in a timely manner to the Board, shared with GIA, or shared with the management of the relevant Baltic subsidiary.

In addition, Clifford Chance reviewed and considered requests from regulators received by Swedbank and its Baltic Subsidiaries regarding AML-related topics and Swedbank's

responses to those requests, to assess Swedbank's transparency when dealing with its regulators regarding such matters. The Investigation found that, in certain instances, Swedbank did not always take an actively transparent posture with regulators regarding AML-related issues, de-emphasized negative information and occasionally employed a narrow or literal reading of certain requests.

Public Disclosures

Clifford Chance considered the completeness and accuracy of Swedbank's public disclosures concerning AML compliance and related issues, in view of the facts established in the Investigation. Specifically, Clifford Chance reviewed public statements made by Swedbank and its executives from January 2014 through March 2019, including for example, interim and annual reports issued by Swedbank and associated materials, other statements and presentations in communications with investors, analysts, and the financial community, corporate debt offering documents and media appearances and publications. When considered in light of the facts developed in the Investigation, certain statements made during October 2018 and February 2019 by Swedbank and its executives concerning Swedbank's historical AML compliance, then current AML compliance, and exposure to certain types of AML risk, were inaccurate or presented without sufficient context.

Accountability

The Investigation also considered which individuals the facts indicated were responsible over time for the existence and perpetuation of the deficiencies in AML and sanctions controls, and why these deficiencies that were identified by GIA, Compliance and other functions, as well as to some extent by Swedbank's external auditors, nonetheless continued without material improvement for many years. In assessing responsibility, the Investigation determined that the three former CEOs who served during the Investigation Period, the Board and certain employees all contributed to a greater or lesser degree to Swedbank's failure to recognize and manage the significant legal and reputational risk to Swedbank posed by its HRNR portfolio in the Baltic Subsidiaries.

As to the CEOs, the Investigation found that the CEO who served from 2009 through 2016 failed to focus on AML deficiencies in the Baltic Subsidiaries during this time despite recurring GIA reports indicating such deficiencies, and notwithstanding an SFSA inspection that found significant AML deficiencies in LC&I and Swedish Banking. With respect to the CEO who served from 2016 through 2019, the Investigation concluded that the CEO's tenure included significant steps to de-risk the HRNR business in the Baltic Subsidiaries and to launch internal investigations of potential AML exposure in response to media reports of money laundering scandals, regulator requests and other indicators. However, the CEO did not direct sufficient resources, attention, or urgency to the remediation of the issues identified, and did not ensure that information regarding these issues was shared between relevant Swedbank control functions or with the Management Boards of the relevant Baltic Subsidiaries. Nor did this CEO ensure that the Board was adequately educated or apprised of the significant legal and reputational risk that these AML deficiencies, in light of the historical high risk customer base in the Baltic Subsidiaries, presented to Swedbank.

As to the Board, the Investigation determined that while the Board was not apprised of the full extent of the legal and reputational risk posed by the AML issues in the Baltics, the Board was informed through regular GIA reports of recurring problems in AML controls, including in the Baltic Subsidiaries. Interviews of Board members indicated that the Board generally understood, based on statements from Swedbank's management, that these matters were under control. Although the minutes of the Audit Committee do reflect relevant discussions of these issues, the full Board record does not reflect significant challenge by the Board to management on the AML issues that were presented to them.

The Investigation also identified a number of employees whose actions and/or inaction caused or contributed to the perpetuation of the AML problems in the Baltic Subsidiaries. These employees ranged from senior managers at Swedbank and the Baltic Subsidiaries, to relationship managers who serviced some of the most problematic HRNR clients, and included members of the customer approval committee in Swedbank Estonia who approved account openings despite apparent red flags. Clifford Chance shared facts regarding these employees with Swedbank over the course of the Investigation, and Swedbank consequently ended the employment of a number of then-current employees.

Remediation

Since the Investigation began in early 2019, Swedbank has appointed a new CEO and a mostly new management team, including a new Chief Compliance Officer (“**CCO**”) and CEO of Swedbank Estonia, and has taken other employment actions dictated in large part by findings in the Investigation. Moreover, Swedbank has a new Board Chair, and the Board now is comprised of mostly new members.

Under this new leadership team, Swedbank has focused on transforming its approach to AML and counter-terrorist financing (“**CTF**”) and sanctions policies and procedures, creating new roles, appointing new personnel, increasing resources, revising and strengthening policies and procedures and taking steps to continue the process of de-risking its customer portfolio including in the Baltic Subsidiaries.

As part of these ongoing de-risking and remediation efforts, and with input from Clifford Chance, Swedbank and its Baltic Subsidiaries have (a) embarked on a much more comprehensive approach and remediation plan to address and to strengthen the AML/CTF and sanctions frameworks; (b) undertaken a review of Swedbank’s corporate governance; (c) engaged external consultants to assist in remediation efforts; (d) increased AML/CTF resources; and (e) continued to off-board customers who do not meet Swedbank’s risk appetite.

In addition, Swedbank is planning to engage a consultant to assess the current state of Swedbank’s AML/CTF policies, procedures, systems and controls, including their implementation. The consultant will identify any existing gaps against regulatory requirements and industry best practices, help Swedbank address those gaps and conduct assessments to ensure that gaps have been fixed.

CLIFFORD CHANCE

Washington, D.C.
Clifford Chance
2001 K Street NW
Washington, DC 20006 - 1001
USA
Tel +1 202 912 5000
Fax +1 202 912 6000

New York
Clifford Chance
31 West 52nd Street
New York, NY 10019-6131
USA
Tel +1 212 878 8000
Fax +1 212 878 8375

Abu Dhabi
Clifford Chance
9th Floor, Al Sila Tower
Abu Dhabi Global Market Square
PO Box 26492
Abu Dhabi
United Arab Emirates
Tel +971 (0)2 613 2300
Fax +971 (0)2 613 2400

Casablanca
Clifford Chance
57, Tour CFC, Casa Anfa,
Hay Hassani, Casablanca 20220
Morocco
Tel +212 520 008 600
Fax +212 520 008 640

London
Clifford Chance
10 Upper Bank Street
London, E14 5JJ
United Kingdom
Tel +44 20 7006 1000
Fax +44 20 7006 5555

Newcastle
Clifford Chance Newcastle Limited
Partnership House, Regent Farm
Road,
Gosforth, Newcastle upon Tyne,
NE3 3AF
Tel +44 20 7006 1000
Fax +44 20 7006 5555

Seoul
Clifford Chance
22nd Floor, D1 Tower,
17, Jongno-3 gil,
Jongno-gu, Seoul 03155
Korea
Tel +82 2 6902 8000
Fax +82 2 6902 8001

Amsterdam
Clifford Chance
IJsbaanpad 2
1076 CV Amsterdam
PO Box 251
1000 AG Amsterdam
The Netherlands
Tel +31 20 7119 000
Fax +31 20 7119 999

Dubai
Clifford Chance
Level 15
Burj Daman
Dubai International Financial Centre
PO Box 9380
Dubai
United Arab Emirates
Tel +971 4 503 2600
Fax +971 4 503 2800

Luxembourg
Clifford Chance
10 boulevard G.D. Charlotte
B.P. 1147
L-1011 Luxembourg
Grand-Duché de Luxembourg
Tel +352 48 50 50 1
Fax +352 48 13 85

Paris
Clifford Chance
1 rue d'Astorg
CS 60058
75377 Paris Cedex 08
France
Tel +33 1 44 05 52 52
Fax +33 1 44 05 52 00

Shanghai
Clifford Chance
25/F, HKRI Centre Tower 2
HKRI Taikoo Hui
288 Shi Men Yi Road
Shanghai 200041
People's Republic of China
Tel +86 21 2320 7288
Fax +86 21 2320 7256

Barcelona
Clifford Chance
Av. Diagonal 682
08034 Barcelona
Spain
Tel +34 93 344 22 00
Fax +34 93 344 22 22

Düsseldorf
Clifford Chance
Königsallee 59
40215 Düsseldorf
Germany
Tel +49 211 43 55-0
Fax +49 211 43 55-6000

Madrid
Clifford Chance
Paseo de la Castellana 110
28046 Madrid
Spain
Tel +34 91 590 75 00
Fax +34 91 590 75 75

Perth
Clifford Chance
Level 7, 190 St Georges Terrace
Perth, WA 6000
Australia
Tel +618 9262 5555
Fax +618 9262 5522

Singapore
Clifford Chance
12 Marina Boulevard
25th Floor Tower 3
Marina Bay Financial Centre
Singapore 018982
Tel +65 6410 2200
Fax +65 6410 2288

Beijing
Clifford Chance
33/F, China World Office 1
No. 1 Jianguomenwai Dajie
Chaoyang District
Beijing 100004
China
Tel +86 10 6535 2288
Fax +86 10 6505 9028

Frankfurt
Clifford Chance
Mainzer Landstraße 46
60325 Frankfurt am Main
Germany
Tel +49 69 71 99-01
Fax +49 69 71 99-4000

Milan
Clifford Chance
Via Broletto, 16
20121 Milan
Italy
Tel +39 02 806 341
Fax +39 02 806 34200

Prague
Clifford Chance
Jungmannova Plaza
Jungmannova 24
110 00 Prague 1
Czech Republic
Tel +420 222 555 222
Fax +420 222 555 000

Sydney
Clifford Chance
Level 16
No. 1 O'Connell Street
Sydney NSW 2000
Australia
Tel +612 8922 8000
Fax +612 8922 8088

Brussels
Clifford Chance
Avenue Louise 65 Box 2
1050 Brussels
Belgium
Tel +32 2 533 5911
Fax +32 2 533 5959

Hong Kong
Clifford Chance
27th Floor
Jardine House
One Connaught Place
Hong Kong
Tel +852 2825 8888
Fax +852 2825 8800

Moscow
Clifford Chance
Ul. Gashheka 6
125047 Moscow
Russian Federation
Tel +7 495 258 5050
Fax +7 495 258 5051

Rome
Clifford Chance
Via Di Villa Sacchetti, 11
00197 Rome
Italy
Tel +39 06 422 911
Fax +39 06 422 91200

Tokyo
Clifford Chance
Palace Building, 3rd floor
1-1, Marunouchi 1-chome
Chiyoda-ku, Tokyo
100-0005
Japan
Tel +81 (0)3 6632 6600
Fax +81 (0)3 6632 6699

Bucharest
Clifford Chance Badea
Excelsior Center
28-30 Academiei Street
12th Floor, Sector 1
Bucharest, 010016
Romania
Tel +40 21 66 66 100
Fax +40 21 66 66 111

Istanbul
Clifford Chance
Kanyon Ofis Binasi Kat 10
Büyükdere Cad. No. 185
34394 Levent
Istanbul
Turkey
Tel +90 212 339 0001
Fax +90 212 339 0098

Munich
Clifford Chance
Lenbachplatz 1
80333 Munich
Germany
Tel +49 89 216 32-0
Fax +49 89 216 32-8600

São Paulo
Clifford Chance
Rua Funchal 418 15th Floor
04551-060 São Paulo SP
Brazil
Tel +55 11 3019 6000
Fax +55 11 3019 6001

Warsaw
Clifford Chance
Norway House
ul. Lwowska 19
00-660 Warszawa
Poland
Tel +48 22 627 11 77
Fax +48 22 627 14 66

*Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.
Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.