

**Danske Bank's written reply to questionnaire from the TAX3 Committee in connection with the public hearing on "Combatting Money-Laundering in the EU Banking system" on 21 November 2018.**

- (1) What are the specific provisions of the Non-Disclosure Agreements (NDAs) Danske Bank's employees in its Estonian branch were required to sign?**
- a. Do these NDA's contain provisions enabling whistle-blowers to share information with authorities and relevant decision makers without fear of reprisal?**
  - b. Do these NDA's make it explicit that reporting on illegal activities is not covered by the NDA?**
  - c. Do the NDA's used by Danske Bank go beyond specific legal requirements to protect the personal information of clients?**

NDAs are generally used to set out and/or highlight a contracting party's obligation to keep confidential the knowledge obtained during the course of the contractual relationship. The NDAs used by Danske Bank in Estonia do not go beyond applicable legal requirements, rather they contain standard clauses commonly used in such agreements. They do not deal specifically with whistleblowing nor do they aim to restrict the rightful use of whistleblowing schemes and rights.

We are in no way opposed to a whistleblower sharing his or hers knowledge about suspicious activities with lawmakers, regulators or authorities including at parliamentary hearings to the extent applicable law makes it possible – on the contrary we would encourage it.

No employee of Danske Bank is prohibited from talking to the police or other authorities if he or she has knowledge about suspicious matters. However, we cannot relieve a whistleblower – or any other employee – of statutory obligations such as the duty of confidentiality in respect of customer matters, specifically where the relevant data is protected and disclosure is prohibited under the banking secrecy provisions of applicable law. These duties are imposed by relevant governing law, not by Danske Bank.

- (2) On which date and in what way was the Danske Bank board of directors made aware of the suspicion of breaches of AML-requirements in the Estonian branch?**
- a. Were individual members of the board, e.g. the chairman of the board, informed in advance of this date, and if so when?**

The Report on the Non-Resident Portfolio commissioned by Danske Bank sets this out in detail, so for a full overview, please refer to the report published on our [website \(danskebank.com/investigations\)](https://danskebank.com/investigations).

Of the findings and conclusions of the report, we can highlight that, up until 2014, reporting on the Estonian branch from Group Compliance & AML to the Executive Board and the

Board of Directors was overall comforting, just as reporting from Group Internal Audit was generally positive.

Following the whistleblower report and conclusions reached by Group Internal Audit, the Audit Committee (but not the chairman of the Board of Directors) received some information in January and April 2014 and the Board of Directors (including the chairman of the Board) also received some information in April 2014. That information was accompanied by assurances that problems were being dealt with and mitigation was ongoing.

**(3) Under which circumstances can executives of Danske Bank be dismissed without compensation?**

- a. Is it failing to inform the board of directors of potential systemic breaches of law in Danske Bank's branches a ground for dismissal of executive staff?**
- b. Has the circumstances surrounding the Estonian branch led to changes in formulation of contracts with senior staff and executives in Danske Bank?**

The possibility of dismissing executives without compensation depends on applicable legislation in the country in question and on the terms of the agreements concluded with each individual executive. In general, a summary dismissal will require that the executive is guilty of gross misconduct and thus has neglected her or his legal obligations under the relevant employment contract and/or regulation.

Danske Bank is improving processes and quality standards on an ongoing basis – so contracts, remuneration policies and governance have undergone several significant changes during the past years. Danske Bank complies with applicable rules on deferral of variable remuneration, back testing and clawback in order to ensure that only sustainable results are rewarded and that members of the Executive Board in Denmark are not entitled to severance pay when their contracts are terminated. Members of the Executive Board are entitled to their normal remuneration during their notice period, however, subject to not having taken up another position.

**(4) According to the “Report on the Non-Resident Portfolio at Danske Bank’s Estonian branch” (Bruun & Hjejle, 19 September 2018) Danske Bank at Group level became aware "[i]n early 2014 (...) that AML procedures at the Estonian branch involving the Non-Resident Portfolio had been manifestly insufficient and inadequate. It was also realised that all control functions (or lines of defence) had failed, both within the branch and at Group level".**

- a. According to the Danish Financial Supervisory Authority (FSA), the board of directors decided in October 2014 to postpone a decision on the Estonian branch to January of 2015. On what grounds did the board of directors reach this decision?**
- b. Did Danske Bank formulate plans to sell-off the Estonian branch or parts of its portfolio in the period between becoming aware of the systemic breaches of AML-requirements and the ultimate closure of activities in 2016?**
- c. Why was the Danish FSA first informed in January of 2015? As per its own report of May 2018.**

First of all, we acknowledge that there were serious failures in this case, for which we take full responsibility. Our controls were inadequate, as was our understanding of the risks involved with this group of customers and our ability to fully comprehend the risk when we received warnings about the non-resident portfolio in Estonia. When it became clear that there were severe breaches of AML procedures at our Estonian branch, we took action. But with the knowledge we have today, it is clear that this action was not sufficient and was implemented too slowly.

We have, and rightfully so, received criticism for not providing sufficient information to the Danish FSA on several occasions up to and including 2017. One reason why it was difficult to share information was that we did not have an overview of the facts and course of events. In hindsight, one of the lessons learned is that we must improve the handling of our dialogue with the Danish FSA. Consequently, we are in the process of establishing a central unit to ensure that we provide adequate information to the Danish FSA with sufficient involvement of the Board of Directors and the Executive Board. We have subsequently, and concurrently with our investigations, shared material with the Danish FSA.

We have also shared with the public the report of 19 September 2018 prepared by Bruun & Hjejle.

Pages 58 to 60 of the report describe the deliberations of the Executive Board and the Board of Directors in relation to the Baltic banking strategy process in 2014 and 2015, which was related to the Baltic banking activities as a whole and not specifically to the non-resident portfolio in Estonia. Various options were considered as part of the strategy and it was decided to reposition the bank towards a Corporate Baltic bank with focus on Nordic

customers. At the time of that discussion, the perception at Group level was that measures had been taken to address the problems identified with the non-resident portfolio in Estonia and that they would be completed during 2014.

**(5) Has Danske Bank in any communication with Mr Wilkinson or his legal representative made mention of their intention to, consideration of or possibility to press charges or initiate legal proceedings based on the provisions of the NDA?**

Danske Bank has not used provisions in any NDAs to prevent anyone from speaking with authorities such as the Danish FSA, the Estonian FSA or the police in this case. It is also important to underline that no employee of Danske Bank is prohibited from talking to the police or other authorities if they have knowledge about suspicious matters pertaining to Danske Bank.

In relation to NDAs, we are not in a position to do anything more than release a person from his or her contractual duty of confidentiality in relation to Danske Bank. We cannot remove the legal obligations any employee must observe, for example the duty of confidentiality in respect of customer matters.

**(6) According to the report prepared by Bruun & Hjejle, Danske Bank failed to nominate an AML responsible person in the period from late 2012 until November 7th 2013, despite this being a clear requirement under Danish law.**

- a. Was the bank at group level aware of this failure to comply with AML provisions?
- b. Was the situation discussed at executive or board level?
- c. Who would have been responsible for the nomination of an AML responsible person?

At the end of 2012, the employee appointed as Danske Bank's AML responsible person retired. Due to an administrative error, a new AML responsible person was not formally appointed until November 2013. The Head of Group Compliance & AML acted as the person responsible for AML activities during that period.

**(7) Russia's central bank reported suspicious transfers in the Estonian branch of Danske Bank already in 2007 to the Danish banking supervisor. Also in 2007, the Estonian banking supervisor published a critical report on Danske Bank. Why did they not lead to thorough inspections? Why did the Bank not take extra measures to carry out CDD?**

As stated in the public report, Group functions in Denmark generally relied on the reports and answers received from the Estonian branch. This included the fact that the Estonian branch had historically had many non-resident customers and that the necessary controls were in place. Group management in Denmark was hence of the perception that the controls necessary to handle the risk posed by the non-resident portfolio were in place.

However, the investigations have clearly demonstrated that this was not the case. Danske Bank failed to react because our control systems and internal reporting did not work as intended. The risks associated with the portfolio were not fully understood. As a result, actions were not taken in due time to respond to the warnings received. This also meant that we did not discover the full extent of the problems in Estonia in due time.

**(8) The Bruun & Hjejle report mentions that employees of Danske Bank may have colluded with customers to get around background and security checks. The Bank stated that it had reported some of its employees and former employees to the Estonian police. Why was that collusion not detected earlier? How is such collusion possible without management's knowledge? How are the criminal procedures progressing? Does Danske Bank blame the employees for acting on their own behalf?**

As the report shows, the internal reporting process was inadequate and the severity of the situation was not fully understood at Group level. The organisation in Denmark did not realise the gravity of the situation in Estonia.

In connection with the investigations, we have reported 42 employees to the Estonian authorities by filing Suspicious Activity Reports (SARs). Eight of these have also been reported to the police. We cannot comment on the progress of criminal procedures, as it is up to the authorities to investigate the reports on suspicious behaviour and possible collusion. What type of collusion and whether there is in fact a link to actual money laundering is for the authorities to determine.

**(9) The investigation on the non-resident portfolio carried out has gone through 6,200 customers starting with customers hitting the most risk indicators. The vast majority of these customers have been deemed suspicious. What was the state of corporate governance at the Bank for this to have happened for years and without serious CDD having been carried out?**

The events that took place in Estonia were not representative of the general state of affairs at Danske Bank. Estonia was the only branch that had a portfolio of only non-resident customers. The non-resident portfolio was closed down in late 2015, with a few remaining accounts closed down in early 2016. The portfolio consisted of high-risk customers, but Group management in Denmark was of the perception that the controls necessary to handle the risk posed by the non-resident portfolio were in place.

At the time, the Estonian branch was not covered by the same customer systems and transaction and risk monitoring as other parts of the Group because it operated on a separate IT platform. That meant that Group management did not have the same insight into the branch as it did into the other parts of the Group. Furthermore, many documents at the Estonian branch, including information about customers, were written in Estonian or Russian.

Danske Bank has since taken steps to improve our anti-money laundering procedures, both in Estonia and at Group level. We are in a different place today when it comes to combating financial crime, and we have taken, and will continue to take, the required measures. The AML area will remain a key priority.

**(10) One of the reasons given in the Bruun & Hjejle report for the banks failure in money laundering checks is the separate IT systems for the headquarters and the Estonian branch. Why were these systems not integrated?**

There are no excuses for what happened in Estonia. The fact that the Estonian branch was allowed to run on a separate IT platform is one of many serious faults in this case.

The migration of the Baltic units to the Group IT platform was planned at the time of the acquisition, but was eventually abandoned on grounds that it was considered too expensive and required too many resources. The risk resulting from allowing a separate IT platform was not realised.

The Baltic units have since been migrated to a shared and integrated IT platform, which ensures a higher degree of transparency and control.