ENFORCEMENT ACTION

Central Bank of Ireland

and

Danske Bank A/S

Danske Bank A/S fined €1,820,000 and reprimanded by the Central Bank of Ireland for transaction monitoring failures in respect of anti-money laundering and terrorist financing systems

On 13 September 2022, the Central Bank of Ireland (the **Central Bank**) reprimanded and fined Danske Bank A/S, trading in Ireland as Danske Bank, €1,820,000 pursuant to its Administrative Sanctions Procedure for three breaches of the Criminal Justice (Money Laundering & Terrorist Financing) Act 2010, as amended (the **CJA**).

The three CJA breaches stem from the failure by Danske Bank A/S (**Danske**) to ensure that its automated transaction monitoring system monitored the transactions of certain categories of customers of its Irish branch[1], for a period of almost nine years, between 2010 and 2019.

The root cause of this failure was historic data filters that were applied within Danske's automated transaction monitoring system, first implemented in 2005 and rolled out to the Irish branch in 2006. Danske failed to consider the appropriateness of these historic data filters within the system or make any adjustments to the system to take account of the specific requirements of the CJA when it came into force in Ireland in 2010. This led to the erroneous exclusion of certain categories of customers from transaction monitoring, including some customers rated by Danske as high and medium risk, which caused the three breaches of the CJA in this case.

In May 2015, Danske became aware, as a result of an internal audit report, of the inadequacies in its transaction monitoring system and the nature of the risks they posed, yet it failed to notify

[1] This included a range of customers, including those categorised by Danske as banks, insurance, stockbrokers and specialised lending customers.

the Irish branch of these issues and to take adequate action for almost four years. It is estimated that between 31 August 2015 and 31 March 2019, 348,321 transactions, equating to approximately one in forty or 2.43% of all transactions processed through the Irish branch were not monitored for money laundering and terrorist financing risk.

The Central Bank has determined the appropriate fine to be €2,600,000, which has been reduced by 30%[2] to €1,820,000 in accordance with the early settlement discount scheme provided for in the Central Bank's Administrative Sanctions Procedure (**ASP**).

This is the first penalty that the Central Bank has imposed on a financial institution which is incorporated and supervised outside of Ireland (i.e. in Denmark) but which operates in Ireland as a branch on a passport basis[3]. The Central Bank has responsibility for Anti-Money Laundering / Countering the Financing of Terrorism (**AML/CFT**) supervision of Danske's branch operations in Ireland.

The three breaches comprised of failures by Danske under the CJA relating to:

- **Transaction Monitoring**: Danske failed to ensure that its automated transaction monitoring system monitored the transactions of certain categories of customer for money laundering and terrorist financing risk at its Irish branch for a period of almost nine years.
- **Enhanced Customer Due Diligence**: In failing to conduct automated transaction monitoring in respect of certain categories of customers, Danske's Irish branch did not take into consideration an important part of due diligence i.e. transaction monitoring data, which is necessary to identify and assess money laundering/terrorist financing risks specific to those customers and identify where any consequential additional measures might be required.
- **Anti-money laundering / Countering the Financing of Terrorism policies, procedures and controls**: The policies, procedures and controls put in place by Danske did not operate to identify the erroneous exclusion of certain categories of customers from automated transaction monitoring.

The three breaches have been admitted by Danske.

[2] Further information is available on the Early Discount Scheme at point 4 of the Notes section.
[3] In this case, Danske is "passporting in" to Ireland i.e. it uses an authorisation obtained in Denmark to sell its products or services in Ireland. The legal entity remains in Denmark, and it operates in Ireland by way of a 'branch'. Further information on 'passporting' is available at point 8 of the Notes section.

The Central Bank's Director of Enforcement and Anti-Money Laundering, Seana Cunningham, said:

"The importance of transaction monitoring in the global fight against money laundering and terrorist financing cannot be overstated. It is imperative that firms implement robust transaction monitoring controls which are appropriate to the money laundering risks present and the size, activities, and complexity of their business. These controls must be applied to all customers, irrespective of their risk rating, as they enable firms to detect unusual transactions or patterns of transactions and where required apply enhanced customer due diligence to determine whether the transactions are suspicious.

The Central Bank recognises that while firms may rely on automated solutions for transaction monitoring, they must ensure that systems employed for this purpose are appropriately monitored, and calibrated correctly to take account of the actual money laundering or terrorist financing risk to which the firm is exposed. In this case, the transaction monitoring system used by the Irish branch was a Danske group wide automated system that had applied historic data filters which operated to erroneously exclude certain categories of customers from being monitored for a period of almost nine years. This led to the serious breaches in this case.

This case highlights the requirement for firms, including those operating in Ireland on a branch basis, to ensure that group systems, controls, policies and procedures are compatible with Irish legal requirements and to ensure that their governance framework and risk management measures operate effectively. These should be risk-based and proportionate, informed by firms' business risk assessment of their money laundering and terrorist financing risk exposure.

Danske became aware that its automated transaction monitoring system erroneously excluded certain categories of customers in May 2015 but failed to rectify it or notify the Irish branch or the Central Bank of this issue. It was only in October 2018 when the Irish branch identified the issue that steps were taken to rectify it, which were completed in March 2019. However, the Central Bank was not informed of the issue until February 2019. The failures to rectify the issue and to notify the Central Bank promptly are aggravating factors in this case. The Central Bank expects firms to bring failures to its attention at the earliest opportunity and to act expediently to address identified errors. The Central Bank will hold firms, including those operating in Ireland on a passporting basis, fully accountable where they fail to take such actions.

Anti-money laundering and countering the financing of terrorism compliance is, and will remain, a key priority for the Central Bank. This case demonstrates our willingness to pursue enforcement actions

and impose sanctions where firms fail in their anti-money laundering/countering the financing of terrorism compliance."

BACKGROUND

Danske is a credit institution incorporated in Denmark and authorised there by the Danish Financial Supervisory Authority (the **Danish FSA**). It is the largest bank in Denmark serving personal, business, corporate and institutional clients and operates in a number of other countries via a branch network.

Danske's Irish branch operates on a 'freedom of establishment' basis i.e. because Danske is established and authorised in Denmark, it is entitled to 'passport' in to Ireland and establish a branch here. The Irish branch is not a separate legal entity to Danske, and it is for this reason that Danske is the named party in the enforcement action. Supervision of the Irish branch sits predominantly with the Danish FSA (as home regulator) but the Central Bank (as host country) regulates it for conduct of business rules and is responsible for supervision of compliance by Danske's branch operations in Ireland with AML/CFT obligations under the CJA.

Danske's Irish branch predominantly provides banking services to large corporate and institutional customers including the public sector in Ireland[4]. Consequently, transaction volumes through the Irish branch, including cross-border funds transfers, are substantial. The Irish branch utilises a group wide automated transaction monitoring system that is implemented and managed by Danske from Denmark.

THE LEGISLATIVE FRAMEWORK

The CJA requires a credit and financial institution to monitor any business relationship that it has with a customer to the extent reasonably warranted by the risk of money laundering/terrorist financing (**ML/TF)**. 'Transaction Monitoring' forms part of a broader system of interconnected elements that comprise a firm's defence against ML/TF and is an important method which assists firms in identifying high risk situations which may require enhanced due diligence on a customer.

Firms are also required to adopt and maintain a system of policies, procedures and controls in relation to AML/CFT, and to monitor compliance with those policies, procedures and controls. Such policies, procedures and controls include, *inter alia*, those dealing with the monitoring of

[4] This includes the Central Bank.

transactions for the identification and scrutiny of any complex, large or unusual patterns of transactions.

THE INVESTIGATION

The Central Bank's investigation confirmed serious inadequacies within Danske's automated transaction monitoring system. Historic filters were applied to Danske's automated transaction monitoring system which erroneously excluded certain categories of customers from transaction monitoring. This led to Danske being in breach of certain obligations under the CJA which gave rise to the three breaches in this case (see below under Prescribed Contraventions for further detail).

The investigation found that the exclusion of certain categories of customers from transaction monitoring was first identified in a May 2015 internal audit report. The May 2015 internal audit report also identified inadequacies with Danske's transaction monitoring policies for certain categories of customers. However, these internal audit findings were not communicated by Danske to either its Irish branch or the Central Bank. Steps were only taken to monitor the transactions of these customers in October 2018 when the Irish branch became aware of the issue, which were completed by the end of March 2019. The Central Bank was not informed of this issue until February 2019.

To illustrate the scale of the failure to monitor, it is estimated that, during the period from 2015 to 2019 when Danske was aware of the issue, 348,321 transactions, equating to approximately one in every forty or 2.43% of all transactions processed through the Irish branch were not monitored.

Danske has confirmed to the Central Bank that by the end of March 2019 it had fully deactivated the erroneous historic filters which gave rise to the breaches in this case. Danske has also confirmed that by April 2020, it completed a third party review exercise for the period 2016 to 2019. Danske has advised that the outcome of the review showed that the risk of suspicious transactions amongst those examined was very low.

PRESCRIBED CONTRAVENTIONS

The Central Bank's investigation identified three breaches of the CJA, as set out below.

Breach by failure to conduct transaction monitoring

Between 15 July 2010 and 31 March 2019 Danske breached sections 30B(1)(a), 35(3) and 36A(1) (as applicable) of the CJA by failing to monitor the transactions of certain categories of

customers for money laundering and terrorist financing risk. The failure meant that the Irish branch was not in a position to:

- Scrutinise these customers' transactions to the extent reasonably warranted by the risk of ML/TF;
- Determine whether any of the unmonitored transactions were complex, unusually large, of an unusual pattern or whether they had an apparent economic or lawful purpose; or
- Identify and assess the risk of ML/TF having regard to the relevant business risk assessment for the purposes of determining the extent of measures to be taken under section 35(3) of the CJA in relation to these customers.

Breach in relation to enhanced customer due diligence measures

Between 14 June 2013 and 31 March 2019 Danske breached section 39 of the CJA on the basis that by failing to conduct transaction monitoring on certain categories of customers, it did not take into consideration an important part of due diligence i.e. transaction monitoring data, which is necessary to identify and assess ML/TF risks specific to those customers and identify whether additional measures were required on these certain categories of customers.

Breach in adopting ML/TF policies and procedures

Between 15 July 2010 and 31 March 2019, Danske breached sections 54(1), 54(2) and 54(4) of the CJA on the basis that the policies, procedures and controls that were in place did not operate to identify the erroneous exclusion of certain categories of customers from transaction monitoring as set out above. The May 2015 internal audit report identified inadequacies with Danske's transaction monitoring policies for certain categories of customers and Danske took some steps in 2015 to address this by introducing a new AML/CFT policy. Nonetheless, certain categories of customers continued to be excluded from transaction monitoring in the Irish branch.

PENALTY DECISION FACTORS

In deciding the appropriate penalty to impose, the Central Bank had regard to the Outline of the Administrative Sanctions Procedure, dated 2018 and the ASP Sanctions Guidance, dated November 2019. It considered the need to impose a level of penalty proportionate to the nature, seriousness and impact of the contraventions.

The following particular factors are highlighted in this case:

The Nature, Seriousness and Impact of the Contraventions

Two of the breaches were ongoing for almost nine years, and the other was ongoing for almost six years. The breaches represent serious weaknesses in Danske's internal AML/CFT controls. Monitoring transactions, ensuring that an important part of due diligence is taken into consideration to identify where additional measures are required, and having effective policies, procedure and controls are critical parts of a firm's internal AML/CFT framework. Danske's failures in this regard in respect of certain categories of customers that transacted through its Irish branch reveal serious weaknesses in these controls.

From its May 2015 internal audit report, Danske became aware of the inadequacies in its transaction monitoring system, the nature of the ML/TF risks that they posed and that it was at risk of non-compliance with legal requirements. Despite this, Danske failed to take adequate action for almost four years or to inform the Irish branch of these internal audit findings. The breaches of the CJA after this point were reckless.

The Central Bank considers that the breaches in this case represent a serious departure from the required standard.

Two Aggravating Factors

Failure to Report and Failure to Remediate promptly

Danske was on notice of the inadequacies in its transaction monitoring system which erroneously excluded certain categories of customer from the time that they were uncovered in the May 2015 internal audit report but it did not report the matter to the Central Bank until February 2019, almost four years later. Furthermore, Danske continued to exclude certain categories of customers from transaction monitoring until March 2019.

The Central Bank views both of these failures as particularly aggravating given the context of increased supervisory engagement it initiated in July 2018 with Danske following media reports of AML/CFT concerns in other jurisdictions in relation to Danske.

Both of these failings are serious aggravating factors in this case.

Other Considerations

The following were also taken into consideration when determining the appropriate sanction:

- The Irish branch's financial position and the need to impose a proportionate level of penalty.

- The need to have an appropriate deterrent impact on Danske and the regulated financial services sector in general.

The Central Bank notes Danske's cooperation in this investigation and this enforcement action against Danske is now concluded.

NOTES

1. The fine imposed by the Central Bank was imposed under Section 33AQ of the Central Bank Act 1942. The maximum penalty under Section 33AQ is €10,000,000, or an amount equal to 10% of the annual turnover of a regulated financial service provider, whichever is the greater.

2. This is the Central Bank's 150th enforcement outcome, bringing the total fines imposed by the Central Bank to just under €300 million.

3. Funds collected from penalties are included in the Central Bank's Surplus Income, which is payable directly to the Exchequer, following approval of the Statement of Accounts. The penalties are not included in general Central Bank revenue.

4. The fine reflects the application of an early settlement discount of 30%, as per the discount scheme set out at pages 24 – 25 of the Central Bank's Outline of the Administrative Sanctions Procedure 2018 which is here: link. Under the 'Early Settlement Discount Scheme', the Central Bank may allow a discount up to a set maximum to be applied to a sanction that it would otherwise expect to be imposed on a regulated entity after considering the sanctioning factors. Any discount applied pursuant to the Early Settlement Discount Scheme will be applied to the overall sanction, which will have been arrived at by reference to the relevant sanctioning factors. Further information on the 'Early Settlement Discount Scheme' is included as an FAQ on the Central Bank website (available here: Link).

5. A copy of the ASP Sanctions Guidance November 2019 is available here: link. This guidance provides further information on the application of the sanctioning factors set out in the Outline of the Administrative Sanctions Procedure 2018 and the Inquiry Guidelines prescribed pursuant to Section 33BD of the Central Bank Act 1942 (a copy of which is here: link).These documents should be read together.

6. Transaction monitoring is a supervisory priority for the Central Bank. Reference was made to its importance in an AML Bulletin issued in October 2020 (available here: Link)

and in a speech given by the Deputy Governor (Consumer and Investor Protection), Derville Rowland in January 2020 (available here: Link).

7. In September 2019, the Central Bank issued the Anti-Money Laundering and Countering the Finance of Terrorism Guidelines for the Financial Sector which is available for download here: Link.

8. Passporting is an EU mechanism which enables banks and financial services companies that are authorised in any EU/EEA state to trade in any other EU/EEA state with minimal additional authorisation. Passporting is possible because all firms operating within the EU/EEA must comply with the same prudential rules and regulations when providing financial products and services. Firms availing of the passporting mechanism to provide services or establish a branch in another EU/EEA state must also comply with national legislative requirements. Further information on 'passporting' is available on the Central Bank website (available here: Link).