Case 7: Danske Bank

Module 7: How Do We Keep Finance Safe and Fair?

Background

Anti-money laundering (AML) and know-your-customer (KYC) requirements are the primary regulatory tools used to prevent the financial system from being used to move illicit funds. As covered in M7L1 (AML/KYC), banks are legally required to verify the identity of their customers, understand the source of their funds, monitor transactions for suspicious patterns, and file reports with national financial intelligence units when something appears wrong. These requirements exist in virtually every jurisdiction and are enforced through substantial penalties.

Danske Bank is Denmark's largest financial institution, with operations across Scandinavia and the Baltics. In 2007, Danske Bank acquired Sampo Bank, a Finnish bank with a branch in Tallinn, Estonia. Estonia, a small Baltic state with a population of approximately 1.3 million, had positioned itself as a gateway for business with Russia and other post-Soviet states. The Tallinn branch came with a portfolio of "non-resident" customers – clients who were not Estonian citizens or residents but used the branch to access the European banking system.

These non-resident customers were the core of what would become Europe's largest money laundering scandal.

What Happened

Between 2007 and 2015, approximately EUR 200 billion (some estimates reach EUR 230 billion) in suspicious transactions flowed through Danske Bank's Estonian branch. To put this figure in context, Estonia's entire GDP in 2015 was approximately EUR 20 billion. The branch was processing ten times the country's annual economic output in questionable flows.

The non-resident portfolio – approximately 10,000 customers – consisted largely of shell companies registered in jurisdictions with weak disclosure requirements: the British Virgin Islands, Panama, Belize, and the Seychelles. The beneficial owners (the real people behind the shell companies) were often Russian citizens, including individuals connected to the so-called "Russian Laundromat" and "Azerbaijani Laundromat" – organised schemes that moved billions in illicit funds from the former Soviet Union into the Western financial system.

The transactions exhibited patterns that any competent AML system should have flagged. Large round-number transfers between related shell companies. Funds arriving from high-risk jurisdictions and immediately departing to others. Customers with no discernible business operations generating hundreds of millions in turnover. These are standard red flags described in every AML training programme and covered in M7L1.

In 2013, Howard Wilkinson, a British employee working in Danske Bank's Estonian trading unit, filed an internal report documenting suspicious activity. His report identified specific customers, described the patterns, and warned that the branch was being used for money laundering at scale. Danske Bank's compliance department in Copenhagen acknowledged receipt of the report but took no meaningful action. Wilkinson was later moved to a different role.

The Estonian Financial Supervision Authority (EFSA) had also raised concerns about the non-resident portfolio as early as 2007, instructing Danske Bank to improve its AML controls at the branch. Danske Bank responded with procedural adjustments that did not address the underlying problem. The EFSA did not escalate to more aggressive enforcement.

The scandal became public in 2018 when Danske Bank published the results of an internal investigation led by the law firm Bruun & Hjejle. The report confirmed that a large portion of the non-resident transactions were suspicious and that the bank's AML controls had been "manifestly insufficient." CEO Thomas Borgen resigned immediately.

Criminal investigations were launched in Denmark, Estonia, France, and the United States. The US Department of Justice and SEC began probes into potential violations of the Bank Secrecy Act (applicable because some transactions were processed in US dollars through American correspondent banks). In

December 2022, Danske Bank pleaded guilty to conspiracy to commit bank fraud in the US and agreed to pay approximately USD 2 billion in penalties. The Estonian branch's licence was revoked.

The Analysis

Danske Bank is a case where every component of the AML framework existed on paper but failed in practice. The bank had a compliance department, a KYC programme, transaction monitoring systems, and a suspicious activity reporting process. None of them worked as intended.

The root causes were organisational rather than technical. The Estonian branch operated with significant autonomy from Copenhagen headquarters. Its non-resident portfolio was highly profitable – generating substantial fees on large transaction volumes – and this profitability created institutional reluctance to scrutinise the clients too closely. Risk management was siloed: the branch reported to different internal structures depending on the topic, and no single person or team had a complete view of the AML exposure.

The whistleblower's report was the clearest test of the bank's internal controls, and the bank failed it. Wilkinson's 2013 report contained specific, actionable information. A functioning compliance culture would have triggered an immediate investigation, potential account closures, and regulatory notification. Instead, the report was acknowledged and filed. This failure connects directly to M7L2 (RegTech) – technology can flag suspicious patterns, but it is useless if the organisation ignores the flags.

The regulatory failures were equally significant. The EFSA identified problems early but lacked the resources and political authority to force action against Denmark's largest bank operating in a small jurisdiction. Danish regulators deferred to the EFSA because the branch was in Estonia. This jurisdictional gap – each regulator assuming the other was responsible – allowed the laundering to continue for years.

The Danske Bank case influenced the EU's push toward a centralised AML authority. In 2024, the EU established the Anti-Money Laundering Authority (AMLA), based in Frankfurt, with direct supervisory powers over the highest-risk cross-border financial institutions – a direct response to the cross-border regulatory failures that Danske Bank exposed.

Discussion Questions

1. Using M7L1 (AML/KYC), identify which specific KYC and transaction monitoring procedures failed at Danske Bank's Estonian branch and explain what a functioning system would have detected.
2. Howard Wilkinson filed an internal whistleblower report in 2013 that was effectively ignored. Evaluate the role of whistleblower protection in financial regulation, drawing on the compliance governance concepts in M7L4 (Model Risk Governance).
3. EUR 200 billion flowed through a branch in a country with a GDP of EUR 20 billion. How could automated transaction monitoring systems (M7L2, RegTech) be designed to flag this type of macro-level anomaly rather than just individual transaction patterns?
4. If you were appointed as the new head of compliance at Danske Bank in 2014 – one year after Wilkinson's report – what organisational changes would you have implemented to address the Estonian branch's AML failures?
5. Could the creation of a centralised EU AML authority (AMLA) prevent a similar scandal, or will jurisdictional arbitrage find new gaps in the regulatory framework?

Further Reading

- Bruun & Hjejle (2018). *Report on the Non-Resident Portfolio at Danske Bank's Estonian Branch.* September 19, 2018.
- Wilkinson, H. (2018). Testimony before the European Parliament's Committee on Financial Crimes, Tax Evasion and Tax Avoidance (TAX3). November 21, 2018.
- US Department of Justice (2022). *Danske Bank Pleads Guilty to Conspiracy to Commit Bank Fraud.* Press Release, December 13, 2022.