Journal of Business, Accounting and Finance Perspectives

Danske Bank—A Smorgasbord of Risks

Patrick McConnell

Affiliation Recently Macquarie University, Sydney, Australia; pjmcconnell@gmail.com

Submitted: 20 February 2020, accepted: 30 April 2020, published: 9 June 2020

Abstract: In September 2018, Danske Bank, the largest bank in Denmark and one of the largest in the Nordic region, published a report which detailed that the bank's board had fallen into lapses in Anti-Money Laundering/Counter Terrorism Financing (AML/CTF) policies at the bank, in particular, within its Estonian subsidiary. The report was devastating in its criticism of AML processes in the Estonian branch, stating that, over a period of several years, "all lines of defence failed" to manage money laundering risks. Soon after the publication of this report, the CEO of Danske resigned, causing the details of the underlying scandal to become public knowledge (although some the issues involved had been aired publicly on a number of occasions previously). It was also revealed that the bank had become the subject of criminal investigations by US authorities. While the events that are covered in the initial report related to failures to manage AML risks, the situation is more complex than merely deficient AML controls in a remote branch. There was a failure to manage a smorgasbord of different types of risks at both the local and group (i.e., headquarters) level, including: strategic risks; technology risks; and especially operational risks. As befits a sophisticated modern financial institution, Danske Bank operates a group-wide enterprise risk management (ERM) framework covering multiple types of risk (credit, market operational, etc.). The fact that the failure to manage the AML risks took several years to come to light casts doubts on the efficacy of their ERM framework and its implementation. Using Turner's case study approach, this paper considers the Danske Bank case from the perspective of operational risk management with a view to identifying lessons that can be learned from the scandal that can be applied to future, large-scale operational risk events.

Keywords: strategic technology risk; Danske Bank; Russian Laundromat; operational risk management; Turner's Six Stages Model

How to cite: Patrick McConnell. Danske Bank—A Smorgasbord of Risks. *J. Bus. Account. Financ. Perspect.*, 2020, 2(3): 17; doi:10.35995/jbafp2030017.

Foreword to Danske Bank Annual Report 2018 (Danske Annual, 2018)

"Danske Bank is one of the largest financial services providers in Denmark and one of the largest financial institutions in the Nordics. As such, **we have a particular responsibility and an obligation to positively impact the Nordic economies and societies by creating long-term value for all our stakeholders.**

Through our shortcomings and failures in Estonia, including our late and inadequate handling of the issues, we have failed to live up to this responsibility. Not only have we disappointed our customers and our employees but also our shareholders and society at large.

This has changed the way the world sees us and has shaken the trust our stakeholders have in us. Many people are asking themselves if we can be trusted to act responsibly, ethically and lawfully.

No issue can be of greater importance than restoring the trust we have lost. [Emphasis added]"

1. Introduction

Danske Bank, the largest bank in Denmark and one of the largest in the Nordic region, is the very model of a successful, modern universal banking corporation, with a solid record of profitability in its chosen markets in Northern Europe. Given its history of prudent, staid banking, it came as a surprise to investors and customers that the bank had been involved in a massive money-laundering scandal.

In September 2018, the Danske board released a report of an inquiry, by an independent legal firm, into the 'Non-Resident Portfolio at Danske Bank's Estonian branch' (Danske Bank, 2018a). This report concluded that, for a period between 2007 and 2015, some 7.5 million payment transactions involving around 10,000 'non-resident' customers that had been handled through the bank's Estonian branch, located in Tallinn, should have been deemed 'suspicious', according to the bank's Anti-Money Laundering (AML) procedures. The report estimated that these transactions involved some EUR 200 billion in value.

On receiving such an adverse report, the board estimated the bank's gross income from these suspicious pavements totalled some DKK 1.5 (EUR 0.2) billion and this was to "be donated to an independent foundation supporting initiatives to combat international financial crime" (Danske Bank, 2018b). This 'donation' was a substantial hit to the bank's annual profit when combined with an order from the Danish Financial Services Authority (DFSA) to increase capital with a DKK 10 billion Pillar II add-on (DFSA, 2018).

Before describing the Danske case in detail, the "six stages" of Turner's Framework for analysing "organisational disasters" (Turner, 1976) are described. This is believed to be the first paper that addresses the Danske scandal using Turner's case study approach. One of the key insights provided by Turner (1976) is that large organisational disasters, and consequential financial and non-financial losses, emerge, or are "incubated", over a long period of time, and it is difficult for those closest to the action to see the disaster emerging.

The paper then describes the background to the case and, using Turner's Framework, describes the sequence of major events that took place over more than a decade that led to the exposure of the AML scandal.

The paper concludes by identifying some lessons that can be learned from the Danske scandal, specifically the role of risk management functions in assisting business managers to identify and mitigate the myriad of issues that give rise to such events.

Before describing the events, however, Turner's Framework for analysing organisational 'disasters' is briefly described.

2. Turner's Framework

In an often-cited work in decision literature, Turner (1976) examined the official reports of a number of 'disasters' from an organisational perspective. Some of the disasters analysed by Turner resulted in considerable loss of life and so cannot be compared to the failures of management that occurred at Danske Bank. However, Turner considered that discussion of such disasters offers "a paradigm for discussion of less tragic but equally important organisational and inter-organisational failures of foresight", such as significant financial losses in major public companies.

Turner (1976) identified a number of "stages" in the "development of a disaster" and "features" that appear to be common to them, which are summarised in Table 1.

Stage	Features Common to Disasters
1. Initial Beliefs and Norms Culturally accepted beliefs and precautionary norms and procedures	Failure to comply with existing regulations
2. Incubation Period The accumulation of an unnoticed set of events which are at odds with the accepted beliefs	(a) Rigidities of belief (b) Decoy phenomena (c) Disregard of complaints from outsiders (d) Information difficulties and noise (e) The involvement of strangers (f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
3. Precipitating Event The event that forces itself to public attention	
4. Onset The immediate consequences of the collapse of "cultural precautions" becomes apparent	
5. Rescue and Salvage The immediate post collapse situation when rescue attempts begin	
6. Full Cultural Adjustment An inquiry is carried out and beliefs are adjusted.	The establishment of a new level of precautions

Source: Turner (1976) Tables 1 and 2, pages 381 and 391.

Table 1 Common features in the development of a disaster.

In his framework, Turner concentrates on the stages of "initial beliefs" and "incubation period" because he argued that it was before the "onset" of disasters that the most significant organisational failures tended to occur. In an observation that is important for banking regulators and management, Turner (1976) pointed out that:

> "**Disasters, other than those arising from natural forces, are not created overnight**. It is rare that an individual, by virtue of a single error, can create a disastrous outcome in an area believed to be relatively secure. **To achieve such a transformation he or she needs the unwitting assistance offered by access to the resources.... of large organisations, and time** [Emphasis added]".

It should be noted that, whereas organisational disasters may appear suddenly and unexpectedly, Turner (1976) found that often, they were "incubated" over a long period of time, during which the unacceptable gradually became acceptable. Fitzsimmons and Atkins (2017) found that "most major accidents incubate for more than three years, with **more than 25 per cent taking longer than eight years to emerge** [Emphasis added]".

In an important observation, Turner (1976) noted that "large organisations" can create large disasters as the "failure to comply with existing regulations" becomes commonplace across the organisation, over a long period. Because of "information difficulties and noise" in very large organisations, critical information gets diluted and ignored as it moves through various organisational levels.

It should be noted that the events described here took over a decade to fully emerge, but along the way, there were, as documented in Appendix A, many 'red flags' that should have been apparent *if managers had been watching carefully enough.*

As shown in Table 1, Turner (1976) identified several 'features' that he found were common to disasters, from organisational rigidity to individuals' failure to appreciate danger. He argued that disasters tend to occur not as a result of some sudden event, but as a consequence of an accumulation of organisational and individual faults that cause a problem, which could have been contained, to grow into a catastrophe. Turner argues that "small scale disasters can be produced rapidly, but **large-scale disasters can only be produced if time and resources are devoted to them** [Emphasis added]".

During the prolonged incubation period of any large disaster, Turner points out that there is a steady accumulation of events that are at odds with the norms of the organisation(s) but which go unnoticed because their importance is not fully appreciated. It is the gradual acceptance of such events that blinds management and regulators to potential problems.

An important aspect of Turner's methodology is the focus on gathering information from official sources, typically independent inquiries and annual reports. Such reports will have some degree of objectivity and, in particular, will not be reliant on the subjective recollections of managers and staff under pressure at the time that the event surfaces. This means, for example, that newspaper articles published as the scandal emerges are not good sources of information, although they do provide some colour for the narrative.

Turner's framework has been used to investigate cases of operational risk events, such as ANZ Bank (McConnell, 2010) and JPMorgan (McConnell, 2014), and Fitzsimmons and Atkins (2017) used Turner's approach to analyse several cases of organisational disasters in large corporations that caused considerable "reputational damage".

3. Background to the Scandal

3.1. Danske Bank

Danske Bank is the largest bank in Denmark and one of the largest in the Nordic region, with a presence in 15 countries, mostly in Northern Europe. In 2018, the bank serviced some three million customers, mostly personal, i.e., retail, but also business customers (Danske Annual, 2018). Danske Bank is regulated by the Danish Financial Supervisory Authority (DFSA) and considered to be one of six systemically important financial institutions in Denmark, and hence "deemed essential to the financial system".

In 2017, Danske Bank posted gross income of some DKK 76 billion (Net Income DKK 48 billion (approx. Eur 6.3 billion)). Over 93% of gross income was generated in the Nordic countries (Denmark, Sweden, Finland and Norway). Another 4% of gross income was generated in the UK (Northern Ireland), where Danske had previously acquired the Northern Bank and the National Irish Bank (which has Danske-branded branches in Ireland). Of particular note here is that Baltic branches (i.e., Estonia, Latvia and Lithuania) contributed only 0.5% of gross income (Danske Bank, 2018a).

As with many large international banks, the Danske Board organised its risk functions in the so-called 'Three Lines of Defence' model (Danske Bank, 2018a):

> "The first line of defence is the business itself, which must ensure correct, legal and expedient operations. The second line of defence is a risk management function that is to identify and mitigate risks and a compliance function that is to check compliance with rules. Finally, the third line of defence is the internal

audit department, which monitors whether the first and second lines of defence identify the problems. Management [and the Board] receives reporting from the three lines of defence on an ongoing basis."

Given the prevalence of this 'lines of defence' model in modern banking, it is disconcerting to find that "all lines of defence failed" (Danske Bank, 2018a).

3.2. Estonian Branch and the Non-Resident Portfolio

In November 2006, Danske Bank announced its acquisition of Finnish-based Sampo Pank and completed the acquisition in February 2007 (Danske Bank, 2018a). Later, in 2008, Sampo Pank in Estonia was formally turned into a branch of Danske Bank.

During the 1990s, there had been "strong economic ties between the Baltic countries and Russia" (Danske Bank, 2018a), and as a result, the Estonian branch had built up a sizeable portfolio of customers who resided outside Estonia, the so-called 'Non-Resident Portfolio'. This portfolio, which over time numbered roughly some 10,000 firms and individuals, was dominated by customers from "the Russian Federation and the larger Commonwealth of Independent States ("CIS"), including countries such as Azerbaijan and Ukraine" (Danske Bank, 2018a).

Organisationally, the Non-Resident Portfolio, consisting of some 3000 to 4000 customers at any one time, was managed by a separate unit, called the International Banking Division (IBD). Until the end of 2015, when it was closed and the Non-Resident Portfolio terminated, this division held a significant share of this overseas business in the local banking system (Danske Bank, 2018a):

> "By the end of 2013, the Non-Resident Portfolio within Danske Bank's Estonian branch held 44 per cent of the total deposits from non-resident customers in Estonian banks (up from 27 per cent in 2007) and nine per cent of the total deposits from non-resident customers in Baltic banks (up from five per cent in 2007)"

The International Banking Division was profitable (Danske Bank, 2018a):

> "The [Estonian] branch had high earnings on Russian and other non-Baltic customers (non-resident customers), whose total volume of payments through the branch was very considerable. For example, 35% of the profit in the branch in 2012 was generated by Russian customers, who made up 8% of the customer base. . . .
>
> Over the nine years from 2007 through 2015, the flow [of payments] converted into EUR for both the approximately 10,000 customers in the Non-Resident Portfolio and the 15,000 customers subject to investigation was approximately EUR 200 billion."

Up until June 2013, employees at the bank had considered initiating similar businesses with non-resident customers in the branch in Lithuania, but the Executive Board rejected these plans.

At this point, it is important to note that payment income dominated IBD profitability (Danske Bank, 2018a):

> "**As regards the Non-Resident Portfolio, the branch took no credit risks of any significance. For the same reason, little capital was allocated to the Non-Resident Portfolio** [Original Emphasis]"

This meant that, *provided operational risks were being managed*, the Non-Resident Portfolio was an almost perfect banking business, with little or no credit risk, and significant fee income, especially from Foreign Exchange (FX) and Payments transactions. As there is 'no such thing as a free lunch', such excessive profits *should* have raised red flags for business, risk and audit managers but appeared not to have done so.

The problem with this financial 'golden goose' (McConnell, 2013) was that operational risks, in particular money laundering risks, were not being managed properly, and there was a disaster waiting to happen.

3.3. The Russian Laundromat

Before considering the Danske case in detail, it is worth describing the business environment in which misconduct first emerged and then thrived. The term 'Russian Laundromat' has passed into popular folklore to describe various schemes used by rich people to launder money from Russia and other ex-Soviet republics (especially, in this context, Azerbaijan and Moldova) to the UK and other western countries, often via tax havens.

In 2014, the Organized Crime and Corruption Reporting Project (OCCRP), a non-profit media organisation providing an "investigative reporting platform", produced a report titled the "Russian Laundromat" (OCCRP, 2014) which claimed:

> "Between 2010 and early 2014, organized criminals and corrupt politicians in Russia moved US$ 20 billion in dirty funds through this laundromat's complex cleanse-and-spin cycle made up of dozens of offshore companies, banks, fake loans, and proxy agents. The process was then certified as clean by judges in the tiny Republic of Moldova. The newly cleaned funds were then spread across Europe."

In 2017, the OCCRP followed up on this initial report with another which gave details of how the 'Laundromat' worked and the people and businesses involved (OCCRP, 2017):

> "Money entered the Laundromat via a set of shell companies in Russia that exist only on paper and whose ownership cannot be traced. Some of the funds may have been diverted from the Russian treasury through fraud, rigging of state contracts, or customs and tax evasion. ... At the other end of the Laundromat, money flowed out for luxuries, for rock bands touring Russia, and on a small Polish non-governmental organization that pushed Russia's agenda in the European Union."

The Laundromat scheme was "ingenious" (OCCRP, 2017):

> "Organizers created a core of 21 companies based in the United Kingdom (UK), Cyprus and New Zealand and run by hidden owners. A number of Russian companies then used these companies to move their money out of Russia. ... All of the core-group companies appeared to be owned by proxies standing in for hidden owners. Even directors and shareholders of the companies were fake".

And the criminals often used 'fake debt' to allow money to be moved from Russia (OCCRP, 2017):

> "To get the money out, the scheme's organizers devised a clever misdirection. They created a fake debt among some of these core shell companies and then got a Moldovan judge to order the Russian company seeking to launder funds to pay that [fake] debt to a court-controlled account".

Having 'cleaned' the money through Moldova, it was a small step to release the money into the international financial system, through respected international banks, such as Danske Bank (OCCRP, 2017):

> "Between 2011 and 2014, the 21 shell companies fired out 26,746 payments from their various [Moldovan bank] accounts. The payments went to 96 countries, **passing almost without obstacle** into some of the world's biggest banks. ... Finally, **payments of laundered money slid easily** into the world's biggest international banks. [Emphasis added]"

The OCCRP (2017) report showed for the first time that Danske Bank was one of the leading conduits for the flow of illicit funds—but other banks were also involved, including other Nordic banks:

> "The Laundromat illustrates that the world's banking system has been impotent, unable to stanch massive flows of illicit money."

After Danske Bank had been forced to launch its own investigation in 2017, the OCCRP (2018) reported on the flow of illicit funds through the Estonian branch.

> "While Danske began its own investigation last September, its senior management is currently facing outrage from Danish politicians as to why the bank did not act more quickly in addressing long-standing concerns over the operations of its Estonian branch."

3.4. AML Regulations

Both Danish and Estonian banking industries are covered by European Union (EU) law, in this case (Danske Bank, 2018a):

> "EU Directive 2005/60 ("Third AML Directive") was implemented into Estonian law on 28 January 2008 in the form of the Money Laundering and Terrorist Financing Prevention Act ("MLTFPA")"

Under this comprehensive directive, financial institutions in the EU are required to (Danske Bank, 2018a):

(1) Perform "customer due diligence" or 'Know Your Customer; when establishing a business relationship with a customer, including "**an obligation to establish the customer's identity** (and, where applicable, the beneficial owner) and to obtain information on the purpose and intended nature of the business relationship";
(2) Conduct ongoing monitoring of the **business relationship with every customer, including scrutiny of transactions**, "to ensure that the transactions conducted were consistent with the institution's knowledge of the customer, the customer's business and risk profile, including, where necessary, the source of funds"; and
(3) Monitor transactions and if there are "reasonable grounds to suspect a customer of engaging in money laundering (or terrorist financing), **this had to be reported to the Financial Intelligence Unit** ("FIU"), that is a public law enforcement agency . . . in the form of a suspicious activity report (SAR) [Emphasis added]"

Obviously, to fully comply with the EU AML Directive, a financial institution would have to create and properly staff the organisations needed to perform and monitor *all* transactions for potential AML activity and to train their staff in doing so. In addition, a financial institution would have to develop the IT systems necessary to identify (and track) potential Suspicious Activity Reports (SARs). This is a non-trivial undertaking for any financial institution, especially an international bank.

While the Estonian branch did make a large number of SARs to the FIU (Danske Bank, 2018a), the information was neither comprehensive nor complete, as described in the following sections.

4. The Danske Money Laundering Scandal

4.1. Before the Event

Figure 1 (here called the Danske Laundromat) summarises the flow of money through Danske Bank that had given rise to the scandal (from top right to bottom left).

As noted above, after the acquisition of Sampo Pank, the Sampo branch in Tallinn, Estonia, serviced a large number of 'Non-Resident' customers residing in ex-Soviet Union countries including Russia, Azerbaijan and Moldova. Periodically, those customers would transmit money to their accounts in the Danske Estonian branch and then send instructions to make transfers to individuals and businesses overseas (Danske Bank, 2018a).

Typically, the transfer instructions from Non-Residents would be merged with instructions from Estonian customers and passed onto the Danske Bank headquarters in Copenhagen. Here, the transfers would be merged with additional instructions from Danish and other European customers and passed onto partner, so-called 'correspondent', banks (McAndrews, 2010) for delivery to the bank accounts of the final recipients, often businesses registered in London, Paris or New York.

However, what if the businesses were not real but in fact merely 'front' companies created to pay and/or receive money, i.e., to money launder?

In some cases, when the money was paid by a fake 'front company' in, say, London, that business would pass the payment (minus a significant fee) along to accounts in tax havens, such as Cyprus or the British Virgin Islands, where, suitably cleansed, the funds would disappear into the global financial system—and with automation through the SWIFT network, the full set of transfers through the different 'hops' could be executed 'end-to-end' in hours, even minutes.

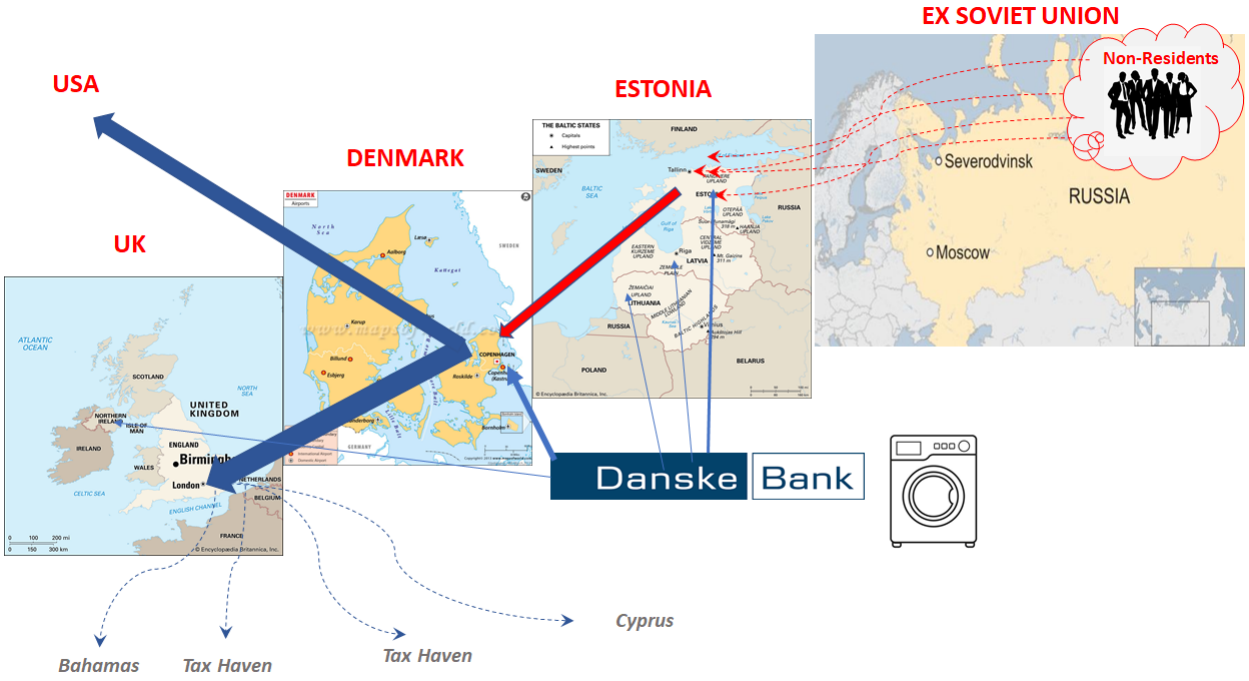

Figure 1 The Danske Laundromat.

It should be noted that almost all of the payments made through these different 'hops' would be totally automated, especially if a Non-Resident customer (even if located outside of the ex-Soviet Union) had used an Internet-banking connection to Danske Bank. This means that staff would have little or no opportunity to catch an invalid transmission as it flows through the system, unless there is an automated AML system for reviewing all transfers and diverting those that look 'suspicious' for further investigation. In addition, good AML practice would also investigate all transfers on a daily, weekly and monthly basis looking for suspicious transactions, patterns and trends. Of course, this can only be done using appropriate computer software that is developed, tested, operated and monitored for compliance according to company policies and regulatory rules.

At this point, it should be recognised that collecting information about the sources and uses of illicit funds is very difficult, as banks, such as Danske, only see part of the overall picture and hence are often unable to verify key information, such as the ultimate owner of a company in a different jurisdiction.

Many international transfers will originate from business customers on a regular basis. For example, an automobile dealer in Russia or Moldova will pay for shipments of vehicles on a regular basis, often using a third-party broker in the West. Thus, assuming that the automobile dealer and third-party broker are bona fide businesses, there would be little need to flag any transfer as suspicious. It would be extremely difficult, for example, to detect if one or more of such payments were suspicious.

However, detailed investigation is *not* what banks are required to do. Under AML legislation, they are required to file a Suspicious Activity Report (SAR) with the appropriate financial intelligence agency—in this case, the Estonian Financial Intelligence Unit (EFIU).

The failure to comprehensively identify suspicious behaviour was highlighted in the analysis of the Non-Resident Portfolio (Danske Bank, 2018a):

> "The SARs filed on the approximately 10,000 customers in the Non-Resident Portfolio **accounted for** approximately **13 per cent** of the total number of SARs filed in the period. [but ...] the Non-Resident Portfolio accounted for **approximately 30 per cent of the total number of FIU inquiries received by the branch** in the period from 2007 through 2015. **Only few of the customers examined have**

> **been deemed not suspicious, that is without suspicious characteristics and not having been involved in payments deemed suspicious**. [Emphasis added]"

In short, almost all activity in the Non-Resident Portfolio, inherited from Sampo Pank and expanded by Danske Bank, should have been considered 'suspicious' *but was not*.

4.2. The Precipitating Event

Turner (1976) identifies two distinct stages that bring a disaster to the public's attention: the "precipitating event", which grabs the attention of the public; and the "onset", or immediate consequences of the event.

In September 2018, the Board of Danske released a report of an inquiry into the 'Non-Resident Portfolio at Danske Bank's Estonian branch', undertaken by an independent legal firm, Bruun & Hjejle (Danske Bank, 2018a). The Board had initiated this inquiry after public and regulatory pressure following publication of details of the Russian Laundromat (OCCRP, 2017).

In a conference call to publish the report, Chairman of the Board of Directors Ole Andersen highlighted the severity of the inquiry's findings (Danske Bank, 2018c):

> "Finally, our investigation shows that the bank has failed to live up to its obligations and responsibility. We, of course, take this very seriously and we regret these events deeply. They do not reflect the kind of bank that we want to be and we'll do everything we can to learn from these events going forward, so that something like this can never happen again".

The remainder of this paper summarises the findings of this and other official reports concerning this scandal.

4.3. The Onset

Turner (1976) identifies a short period after the Precipitating Event, the Onset, during which the "immediate consequences of the collapse of "cultural precautions" become apparent" and in many ways set the scene for what follows.

In the Danske case, the initial reaction was for the CEO, Thomas F. Borgen, to resign, and this was followed pretty quickly by a 'spill' of a number of Board positions, including the Chairman and Chair of the Audit Committee. An internal manager, Jacob Aarup-Andersen, who was not directly involved in the scandal, was proposed as the new interim CEO (Danske Bank, 2018d).

4.4. After the Event

Turner (1976) identifies two final stages that are common in an organisational disaster. In the immediate aftermath, there is the "rescue and salvage" of anything of value left from the disaster, and finally, there is the "cultural adjustment", which attempts to learn lessons from the unhappy events. Again, these stages were apparent in the Danske case.

4.5. Rescue and Salvage

Shortly after the new interim CEO was installed, Danske announced the bank's financial results for the first nine months of 2018, which showed a slight fall in operating income compared to the same period in 2017, but in addition, the Board announced that income was down (Danske Bank, 2018b):

> "as a result of our decision to donate DKK 1.5 billion, corresponding to the gross income from the Estonian non-resident portfolio, to initiatives aimed at combating financial crime."

Interestingly, the Board had attempted to wipe the slate clean by taking a substantial hit to its profits, counteracting any charges that the bank had profited from its mistakes.

However, the bank announced that it had become the subject of criminal investigations by US authorities, which lays the ground for further possibly large regulatory fines in the future (McConnell, 2015).

In considering the case, the bank's main regulator, the Danish Financial Services Authority, considered action under Danish law against staff and management but demurred (DFSA, 2018).

"The Danish FSA has assessed whether there are grounds for bringing actions under the fit and proper rules against the bank's current members of management and staff. On the available basis, the Danish FSA does not consider that there are sufficient grounds for bringing such actions."

However, the DFSA noted that (DFSA, 2019):

> "In Danske Bank's Estonian branch, there have been significant violations of the European and Estonian money laundering rules. In December 2018, ten former employees in the branch were arrested in Estonia. By all accounts, for a number of years employees in the Estonian branch actively carried out and covered up the violations both to the bank's senior management in Copenhagen and to the Estonian Financial Supervisory Authority (EFSA)."

At the time of writing, in late 2019, there are several legal investigations taking place in a number of jurisdictions, and doubtless, further actions will be taken by regulators and other authorities in the future.

4.6. Cultural Adjustment

Turner (1976) points out that after the dust settles, it is possible to carry out a "more leisurely and less superficial assessment" of the events leading up to a disaster, with the goal of learning lessons from it and ultimately closing the circle by adjusting the erroneous beliefs and norms that lead to the failure.

In the Danske case, this included making significant improvements to its operational risk management (ORM) processes, in particular working on AML (Danske Bank, 2018a).

> "The bank has stated that it has increased the number of employees working with AML in the first and second lines of defence from less than 200 to 550 last year and nearly 900 today. Among other things, the bank has also expanded and updated internal AML training, worked to strengthen the compliance culture and made considerable investments in IT in the area."

5. Before the Event

5.1. The Incubation Period

Turner (1976) considered the "incubation period" to be of utmost importance when analysing corporate disasters, as it is actions prior to the "onset of the event" that ultimately determine the "scale" of the organisational disaster. During the incubation period, Turner (1976) points out that there is a steady accumulation of events that are at odds with the norms of the organisation but go unnoticed because their importance is not fully appreciated. Turner identifies the "incubation period" as the stage where the "failures of foresight" that lead to the eventual disaster occur and he describes a number of key features, summarised in Table 1 above, which are common to the disasters that he studied.

Describing Turner's approach, Fitzsimmons and Atkins (2017) noted that:

> "Analysing these long incubations, Turner found steady accumulations of tell-tale events that were not acted upon. Some were overlooked or misunderstood for reasons ranging from wrong assumptions to a failure to understand the complexity of the system. Others were ignored because people refused to accept just how bad the consequences could have been if the mishap had not been a 'near miss'".

The events that led to the Danske scandal coming to the public's attention took place over 12 years during a period of enormous changes in the financial system, most notably the Global Financial Crisis (GFC) of 2007/2008, the impact of which has not completely worked its way out of the global financial system in 2019 (McConnell and Blacker, 2011).

During this prolonged period, there were very many events, actions and inactions by Danske Bank directors, management and staff and also external banking regulators and other financial institutions. Table A1 in Appendix A lists a timeline of some of these events and activities, organised by date, which is broken down in the table by seven distinct phases.

(1) **Strategic Euphoria**: a period of euphoria as the bank's growth strategy in the Baltic countries was implemented (roughly 2006–2008);
(2) **Regulatory Unease**: a period during which banking regulators expressed unease about the implementation of Danske's growth strategy (roughly 2009–2013);
(3) **Management Myopia**: a period during which management appeared to ignore the increasing signs of problems with the growth strategy (roughly 2013–2014);
(4) **Management Tinkering**: a period during which management took steps to ameliorate (some of) the symptoms without really addressing the serious problems emerging (roughly 2014–2016);
(5) **Management Investigations**: a period during which management initiated multiple investigations but did not directly address the problems (roughly 2016–2017);
(6) **Scandal Emerges**: a period during which the full import of the scandal emerged and corrective actions began to be taken (roughly 2017–2018); and
(7) **Aftermath**: a period during which the firm and its regulators began to take actions to attempt to correct the problems that arose during the scandal, also called "Cultural Adjustment" by Turner (1976).

The remainder of this section considers some of the more important events that went unnoticed or were given insufficient attention by management. However, at this point, it should be noted that the events described here were selected, from a vast amount of information, by the author as being important. It is not infeasible that another researcher might select different, even contradictory, events when analysing the events from another perspective.

5.2. Initial Beliefs and Norms

Turner (1976) argues that a disaster or "cultural collapse" takes place because of "some inaccuracy or inadequacy in the accepted norms and beliefs" of a firm or, here, a group of semi-independent branches. Organisational disasters build up gradually over time, and the signs should be apparent to management and regulators. Instead, the warning signs go unnoticed or ignored because of "cultural rigidity" which manifests itself in erroneous assumptions and reluctance to face unpalatable outcomes (Turner, 1976).

In 2006, as it was about to acquire Sampo and its Estonian subsidiary, Danske Bank was very clear in its vision and mission and its strategic positioning (Danske Bank, 2018a).

> "Danske Bank Group focuses on conducting conventional banking business in the northern European markets based on state-of-the-art technology. The Group is a leading player in the Nordic markets."

The Board had developed an overall vision of 'One platform—exceptional brands' based on shared technology (Danske Annual, 2006):

> "We have developed a **solid and scalable platform** to support our core business. The platform consists of systems to manage IT, product development, communications, branding, credits, risk, HR development and finances. **This platform allows all our units across borders to base their work on the same business model.** We continually develop our business model through best practice activities and an active pursuit of new business opportunities. Our ambition is to build and maintain unique brands that respect our core values. [Emphasis added]".

It was very much a vision of a global organisation directed from the centre in the bank's headquarters in Copenhagen, Denmark with:

> "Group standards for risk management, financial planning and control, credit approval, HR development, compliance and the shared IT platform ensure a well-structured management of all activities."

While there is nothing intrinsically wrong with such a vision and aspirations, the difficulties of actually implementing common standards across diverse markets and cultures must be recognised. Such a vision is replete with strategic implementation risks (McConnell, 2016).

5.3. Rigidities of Belief

Turner (1976) points out that all organisations develop a culture that relates the tasks that individuals perform to the goals of the firm and that success stems from the effectiveness of that culture. The other side of this coin, however, is that in attempting to create an all-pervasive culture, managers may well become blind to potential problems outside of the perceived norms. Turner (1976) describes how, in the development of a disaster, important events go "unnoticed or misunderstood because of erroneous assumptions".

In the case of Danske Bank, an erroneous assumption was that whenever a policy was agreed at board and headquarter level, it would be implemented throughout the bank organisation as 'one platform'. While such an assumption *may have been* valid when Danske was based mainly in Denmark and was staffed primarily by Danes, it does not necessarily hold as the bank acquired new staff in countries with different cultures, and existing work practices.

This is not a judgement on non-Nordic countries, but merely that distinct differences in organisational cultures have been observed between countries (Hofstede, 1991). Even without delving too deeply into Hofstede's six dimensions of national culture, it should be apparent that approaches to organisational compliance would almost certainly differ between a Western European democracy and a country and people still emerging from Soviet dominance. There is no evidence that Danske considered that different approaches to compliance might be needed, if only in communicating policies, in their recently acquired ex-Soviet subsidiaries.

5.4. Decoy Phenomena

In describing the 'decoy phenomenon', Turner (1976) noted that:

> "A recurrent feature of the reports analyzed is that in many instances, when some hazard or problem was perceived, action taken to deal with that problem distracted attention from the problems which eventually caused trouble".

In the case of Danske, there was a huge 'decoy phenomenon', that of the Global Financial crisis (GFC), which occurred just a few years into the acquisition of Sampo Pank and, in particular, it was not surprising, given the problems in the Irish economy at the time (Nyberg, 2011), that the bank's board focussed on its Irish and UK investments. In the great scheme of things, the relatively 'minor' operational issues in the Estonian branch would not reach the top of the pile of important problems that needed to be resolved quickly.

5.5. Disregard of Complaints from Outsiders

Perhaps one of the most surprising findings in the disasters reported by Turner (1976), Gleick (1992) and Augustine (1995) was that often there were clear warnings of potential danger before a disaster occurs. However, warnings from outsiders were routinely dismissed by management with the assumption that the firm knows better than outsiders as to how to run its business.

The same "organizational exclusivity"[1] was apparent within Danske Bank, especially in respect of warnings from external parties:

(1) Warnings from financial regulators;
(2) The termination of major 'correspondent' banks from their long-standing business relationship with Danske Bank; and
(3) The failure to take seriously a 'whistle-blower complaint' from a senior staff member working in the Estonian branch.

5.5.1. Warnings from Financial Regulators

Given the international emphasis on banking regulation (Bank for International Settlements, 2004), it is hard to believe that any major bank would not take their regulators' concerns seriously. However, as shown in the timeline in Appendix A, Danske Bank's management appeared to play down concerns from a number of financial regulators over the decade, during which the AML problems were documented, but not properly addressed.

First, and in hindsight most surprisingly, the bank appears not to have taken seriously warnings from the Russian Central bank in 2007 when Sampo Pank was acquired (DFSA, 2019):

> "The Russian central bank warned the Danish FSA about AML risks related to a number of Russian customers in Danske Bank's newly acquired Estonian subsidiary."

This warning was obviously passed onto Danske, where an investigation was undertaken (DFSA, 2019):

> "The feedback received from both [heads of Legal and Audit] was that **there were no problems in relation to AML risks in the Estonian subsidiary** [Emphasis added]."

Additionally, in 2007, as the Estonian branch was being acquired, the local regulator, the Estonian Financial Services Authority (EFSA), also warned the Danish regulator and the bank (DFSA, 2019):

> "The EFSA found deficiencies in relation to the subsidiary's management of AML risks and on that basis issued an order for the subsidiary on further measures to investigate new non-Baltic customers (non-resident customers) and to strengthen internal AML procedures".

However, investigations appeared not to have uncovered the full extent of the problem (DFSA, 2019):

> "However, neither Danske Bank nor the EFSA identified problems on a scale anywhere near what was later identified."

Obviously, a golden opportunity to nip the AML problem in the bud had been missed not only by Danske Bank but also their regulators in Denmark and Estonia. Although regulators may have missed the full import of the problem, the ultimate responsibility, of course, resided with the Board of Danske Bank.

In 2009, the Estonian financial regulator again conducted an AML inspection which gave a modicum of comfort to Danske Bank directors (DFSA, 2019):

> "EFSA also concluded that EFSA had found some weaknesses, but did not find serious shortcomings or problems, and that the problems identified in 2007 appeared to have been handled."

Again, another opportunity to delve into and resolve 'weaknesses' was missed and, instead, over the next 3 years or so, the number of Non-Resident customers grew, as did the number of 'suspicious transactions'

In 2012, the Danish regulator (DFSA) undertook an inspection of processes at Danske Bank and concluded that "**Danske Bank has historically not lived up to its obligations in the AML area** [Emphasis added]" (DFSA, 2018).

In 2013, the Estonian FSA contacted the Danish FSA about possible AML issues at the branch, alleging that "**detailed information** from 2012 and 2013 to the Danish FSA and the Estonian FSA therefore **was misleading** [Emphasis added]".

On inspection, the Danish regulator discovered that (DFSA, 2018):

"From the end of 2012 to November 2013, Danske Bank did not have a person responsible for AML activities as required by the Danish Anti-Money Laundering Act."

Technically, this meant that Danske Bank was in violation of Danish law at that point and had been so for some time.

In 2013, regulatory investigations began to heat up (Danske Bank, 2018a):

"The EFSA contacted the Danish FSA again regarding AML risks in the Estonian branch. The inquiry was based on a warning from the Russian central bank which included a list with a number of the branch's Russian customers, which the Russian central bank considered to be suspicious, and on the EFSA's own analysis of the branch's customer mix."

However, Danske Bank management again appeared to downplay the problems (DFSA, 2019):

"The Danish FSA asked Danske Bank to address EFSA's request. The bank's acting Head of the Legal Department replied that the Estonian branch had a special setup in the light of the elevated AML risk in the branch."

Additionally, the bank appears to not have been thorough and diligent in its response (DFSA, 2019):

"However, the evidence shows that the **bank did not always provide the FSA with accurate information,** and that in several cases this was due to **the bank not being sufficiently thorough in its** investigation of the facts before replying to the Danish FSA [Emphasis added]."

Towards the end of 2013, the bank's management received a report from a whistle-blower, as described in the next section, which seemed to confirm regulators' concerns. In 2014, the Estonian regulator (DFSA, 2019):

"conducted two AML inspections in 2014. The Danish FSA was not asked to attend. The inspections **showed significant weaknesses in the branch's AML procedures** and led to orders from the EFSA and **the** replacement **of the branch's local management.** [Emphasis added]"

A senior employee emailed colleagues concerning the EFSA report (DFSA, 2019):

"The executive summary of the Estonian FSA letter is brutal to say the least and is close to the worst I have ever read within the AML/CTF area (***and I have read some harsh letters***). [Emphasis added]".

However, the Danske Board and management appeared still not to be fully aware of the seriousness of the situation, failing to take seriously the regulator's warnings (Danske Bank, 2018a):

"the Estonian FSA's critical conclusions were thus still toned down in the minuted discussions of the Executive Board and in written internal reporting to the Board of Directors."

In 2015, after further warnings from the Estonian regulator, the Danske Board eventually began to act, ordering that the Non-Resident portfolio be closed down, but "another year passed before, in January 2016, the close down was completed" (DFSA, 2019).

In March 2017, the Russian Laundromat investigation was reported in the press (OCCRP, 2017), implicating Danske Bank in money laundering activities. At that point, stung by media pressure, the Danish regulator began an investigation and asked "the bank's Board of Directors and Executive Board for a written statement about this case and more generally about AML handling at the branch" (DFSA, 2019).

The Danish regulator was not, however, completely satisfied with the information supplied by the bank (DFSA, 2019):

"**As a result of inadequate information being provided to the Danish FSA**, the Danish FSA has found it necessary to enquire more than once regarding the same issues in order to receive an adequate reply and to enquire about the bank's knowledge of further cases. [Emphasis added]"

Finally, in September 2017, *a full decade after the first warnings from the Russian Central Bank*, the Danske Bank Board acknowledged that (Danske Bank, 2017):

> "**major deficiencies in controls and governance** that made it possible to use Danske Bank's branch in Estonia **for** criminal **activities such as money laundering** [Emphasis added]".

At that point, the external investigation (Danske Bank, 2018a) was initiated which led to the events that resulted in the resignation of the CEO and Chairman and the reorganisation of the organisation, as described above.

When the interactions are laid out in the sequence above and documented in Appendix A, it is difficult to believe that the warnings from the bank's senior regulators were ignored and/or downplayed. That is hindsight, though.

As Turner (1976) observes, prior to many organisational disasters, there was a "failure to comply with existing regulations", with those closest to an impending disaster unable to see the looming crisis because of "cultural rigidity". Danske Bank's Board and management had a "blind spot" (Blacker and McConnell, 2015) as regards money laundering, obviously not fully aware of the importance placed upon the crime by overseas authorities.

5.5.2. Termination of Correspondent Bank Relationships

Because the costs of setting up a fully-fledged overseas banking operation to support their largest clients are so enormous, banks often enter into what is called a 'correspondent banking' relationship with overseas banks (McAndrews, 2010). For example, in order to process payments in US dollars for a client, such as Maersk, i.e., one of the world's largest shipping companies, Danske Bank would typically set up a legal arrangement with a local US bank, such as JP Morgan. For a fee, JPMorgan then would accept and make payments on behalf of Danske Bank, and Danske Bank would agree to do the same for clients of JP Morgan with business in Denmark.

Today, international commerce is driven through complex networks of mutually beneficial correspondent banking relationships between the largest banks in each country/jurisdiction. These correspondent networks are, in turn, aided by highly automated global communications networks, such as SWIFT (McAndrews, 2010).

Although driven by opportunities for profit, any particular correspondent relationship between two banks is based on '**trust**'; trust that the receiving bank will execute a banking transaction to the best of its capabilities; and trust that the sending bank will only request legal transactions, as the receiving bank will have legal liability for illegal transactions in their home jurisdiction.

This is particularly important for any payments transactions that are subject to Anti-Money Laundering controls in that the receiving bank may be judged as being liable for any transgression of AML laws *in their local jurisdiction.*

In a somewhat anomalous situation, the Danske branch in Estonia had its own direct correspondent banking relationship for making USD payments. However, in June 2013 (Danske Bank, 2018a):

> "a member of the Executive Board was contacted by one of the bank's correspondent banks with a view to terminating the correspondent banking relationship on grounds of AML."

Despite this serious matter being raised with the highest level of the bank, the warning appeared not to have rung alarm bells sufficiently and, after an internal review, the relationship was terminated *but* immediately replaced by another, different relationship (Danske Bank, 2018a).

In 2015, two separate correspondent banks in the USA approached Danske at 'group level' with warnings concerning transactions emanating from the Estonian branch, and one bank is reported as stating (Danske Bank, 2018a) that they:

> "did not want to go into detail, but made it clear that they had found some payments that they were not comfortable with".

A review at the time, by the bank's Group Compliance and AML team, warned (Danske Bank, 2018a) that "we should be mindful that we **have a really bad case in Estonia**, where ... **all lines of defence failed** [Emphasis

added]". However, these warnings and the terminations of major banking correspondent banking relationships with the Estonian branch were not reported to the Board.

At the very least, the termination of major correspondent banking relationships should have raised 'red flags' in all management, risk and compliance forums. However, it appears that while some unease was felt, no significant actions appear to have been taken to get to the bottom of the reasons such important relationships were terminated.

5.5.3. The Danske Whistle-Blower

In 2012, a senior employee in the Estonian branch felt that "he had no option but to approach senior group employees directly" because (Danske Bank, 2018a):

> "It is not appropriate to raise these issues within the branch due to their serious nature, that it is unclear at what level in the branch there was knowledge of the incident and because of a general problem regarding confidentiality in the branch."

After doing some basic research (at the UK Companies House), the whistle-blower discovered that a particular UK company, which was receiving large payments, was in effect a dormant company with little business activity other than receiving and then disbursing payments from accounts of 'non-residents'. In a damning report, he concluded that (Danske Bank, 2018a):

> "**The bank may itself have committed a criminal offence;** The bank can be seen as having aided a company that turned out to be doing suspicious transactions (helping to launder money?); **The bank has likely** breached **numerous regulatory requirements.** The bank has behaved unethically; and **There has been a near total process failure.** [Emphasis added]"

Reaction to the whistle-blower's report was slow, taking more than a year for the suspicious customer relationship to be terminated. This was because the whistle-blower was initially viewed with suspicion, as he decided to bypass the normal branch-based whistle-blowing process, voicing his concerns directly to headquarters where, of course, he was considered an 'outsider' who was circumventing standard procedures.

In 2014, the Danske Bank Group's internal audit department (GIA) conducted several AML audits at the branch, which "**confirmed significant AML deficiencies as pointed out by the whistle-blower** [Emphasis added]", especially that companies were being set up, with complicated opaque ownership corporate structures specifically "to avoid submitting financial statements" and with beneficial owners that were not "known by the bank, or were known but not registered in the relevant systems of the branch" (Danske Bank, 2018a)—all clear contraventions of the EU AML regulations.

In a damning analysis of the bank's failure to address the extremely serious issues raised, the independent review stated (Danske Bank, 2018a):

> "In the period after the whistle-blower report, there were several indications that members of the management and/or employees of the branch **were colluding with non-resident customers in criminal activities or, at least, knew of such activities**. The bank did not, however, investigate this, and there were **no managers or employees who were dismissed or relocated because of such a suspicion**. [Emphasis added]"

The failure of senior management and group control functions to act on the serious issues raised by reputable correspondent banks and the senior whistle-blower illustrates that bank management disregarded complaints from those not in the 'inner circle' because "it was automatically assumed that the organizations knew better than outsiders about the hazards of the situations with which they were dealing" (Turner, 1976).

5.6. Information Difficulties and Noise

Banking is an information-intensive industry (McConnell, 2017). Every day, in any large financial institution, such as Danske Bank, millions of pieces of information are captured from banking transactions, such as payments, deposits, mortgage repayments, Foreign Exchange trades and so on. These captured data are stored, processed, aggregated and reported to customers (as statements), regulators (as regulatory repots) and to management as information of many different types (operating volumes, profitability, risks, future liabilities etc.) While the vast majority of this information will be 'correct', an unknown proportion will be incorrect—the result of genuine mistakes, delays and even fraud.

Finding these errors, however, is like finding the proverbial needle in a very large haystack, and even harder as the haystack is continually growing and shifting shape. Furthermore, after anomalies are found, selecting the errors in order of importance is also very difficult.

Of course, modern banks use Information Technology (IT) to perform the vast bulk of the job of searching for, and reporting, potential errors. Banking and most other businesses today are driven by 'exception reporting' or the highlighting of possible exceptions in a vast mass of data. If IT systems have not been programmed to pick up exceptions, then management and ultimately a board will be making decisions on the basis of incorrect, out-of-date or incomplete information.

As noted earlier, Danske Bank Management were very proud of their 'One Platform' strategy (Danske Annual, 2007):

> "We have developed a solid and scalable platform to support our core business. The platform consists of systems to manage IT, product development, communications, branding, credits, risk, HR development and finances. **This platform allows all our units across borders to base their work on the same business model** [Emphasis added]".

By having a single and shared IT platform across all (or almost all) business units, management information can be produced that is 'consistent', providing the basis for identifying exceptions that management needs to address.

In late 2006, announced the acquisition of Sampo Pank and noted (Danske Annual, 2006):

> "Danske Bank expects to complete the integration of Sampo Pank's Finnish activities on its IT platform at Easter 2008. It has not yet been decided when to integrate the still relatively small operations in Estonia, Latvia, Lithuania and Russia."

It should be noted that the announcement stated "*when*" not "*if*" the Estonian branch would be integrated into the 'One Platform', and as a measure of whether this was achievable, and indeed what had been achieved, the report added:

> "The Group vision of creating "one platform—exceptional brands" was clearly reflected in the successful migration of the systems of National Irish Bank and Northern Bank to the Group's shared IT platform during Easter 2006."

However, unlike the situation in the Irish banks, the integration of the Baltic branches of Sampo, especially Estonia, did not go well for reasons that were not expanded upon (Danske Annual, 2008):

> "In the third quarter of 2008, on the basis of a cost analysis, the Group **decided to discontinue the migration of Banking Activities Baltics to its shared IT platform**. But this will not stop future investments in the Baltic banks and their IT departments and local IT systems. The Group will also continue the business integration of the banks and will market Danske Bank products where relevant. [Emphasis added]".

In other words, the IT systems used to capture and, more importantly, to report to Group management and the Board were not consistent across the bank, giving rise to considerable "difficulties and noise" (Turner, 1976).

In particular, in the context of this case, the identification of 'suspicious' money laundering transactions was not consistent and indeed may have been downplayed, or even removed, in the alternative Estonian systems.

With hindsight, the decision not to complete the integration of the Baltic branches, ostensibly for cost reasons, cost the bank very dearly.

5.7. The Involvement of Strangers

Turner refers to "strangers" as members of the general public who may behave unpredictably in a disaster. In Turner's framework, 'strangers' may not necessarily contribute directly to the causes of disasters but become part of the 'noise' that distracts the attention of the participants and hinders the detection of potential problems. In the Allied Irish Bank (AIB) and National Australia Bank (NAB) cases, McConnell (2003, 2005) identified examples of 'strangers' in the banking industry, in particular brokers, who had an impact on those events.

In the Danske case, the 'strangers' are obvious—they are the firms and individuals who were classified as the 'Non-Resident Portfolio'. It was the failure of the bank's employees and managers to get to 'Know Your Customers' (KYC) that led to the scandal and considerable cost to Danske Bank, not only in money but also in reputation.

The number of these strangers is significant, estimated at "approximately 10,000 in the period from 2007 through 2015", including some customers that were "passive" (Danske Bank, 2018a). At any one time, Danske Bank (2018a) documents that there just under 3900 active customers with customers coming and going from different jurisdictions (even a small number from Estonia itself):

> "Over time, the geographical distribution of the customers in the Non-Resident Portfolio changed. In total, customers came from 90 countries based on their registered or recorded residency status (for example, postal address for private persons and country of incorporation for corporate entities), the three main countries being Russia, the UK and the British Virgin Islands."

It should be noted that changes in the numbers and origins of customers would be expected in a money laundering situation, as criminals attempt to stay ahead of their pursuers—here, the financial crime authorities. Danske Bank (2018a) provides copious statistics on the make-up of the Non-Resident Portfolio over time, and it should also be noted that there were approximately 5000 customers who resided outside of Estonia, such as in other Nordic countries, who were not considered to be part of the Portfolio.

These strangers/customers were very active in making significant payments (Danske Bank, 2018a):

> "In the period from 2007 through 2015, the approximately 10,000 customers in the Non-Resident Portfolio had approximately 7.5 million incoming and outgoing payments. . . . . The flow as converted into EUR was approximately EUR 200 billion."

It was the failure to comply with AML regulations for many of these payments that created the scandal and cost Danske dearly.

5.8. Failure to Comply with Discredited or Out-of-Date Regulations

Turner (1976) documents how, prior to many organisational disasters, there was often a "failure to comply with existing regulations", with those closest to an impending disaster unable to see the looming chaos because of so-called "cultural rigidity". In this case, the "existing regulations" ignored were those of regulators who had developed rules as to how AML activities should be identified and reported to financial crime authorities.

It should be noted that the term 'discredited or out-of-date regulations' refers to the perceptions of management *not* regulators, as there is no evidence that the various regulators for Danske downplayed the importance of AML as illustrated above when discussing complaints from regulators. The independent report found that (Danske Bank, 2018a):

> "AML procedures at the Estonian branch in relation to the Non-Resident Portfolio were manifestly insufficient and inadequate and in breach of international standards as well as Estonian law. This was so even though the **non-resident customers were categorised as high risk.** [Emphasis added]"

The report listed, in great detail, some very clear examples of non-compliance and failures of due diligence, including clear breaches of AML regulations (Danske Bank, 2018a):

- "Lacking knowledge of customers;
- Lacking identification of (ultimate) beneficial owners and "controlling interests";
- Customers included so-called intermediaries, which were unregulated and represented; .
- Insufficient attention to customer activities;
- Lacking identification of the source and origin of funds used in transactions;
- No screening of customers against lists of politically exposed persons;
- No screening of incoming payments against sanctions or terror lists"; and
- Several other clear failures of AML monitoring and reporting.

There were also serious organizational failings:

> "Other shortcomings have been identified, such as the **lack of independence between the AML function** at the Estonian branch and the business and **insufficient training of the staff** of the Estonian branch and **lack of formal procedures**. [Emphasis added]"

Furthermore, in addition to the manifest failures as regards AML compliance, the firm appeared to be in breach of its obligations with the Danish regulator (Danske Bank, 2018a):

> "From the end of 2012 to November 2013, Danske Bank did not have a person responsible for AML activities as required by the Danish Anti-Money Laundering Act. The Danish FSA was not notified of this until February 2018 and then as a result of the Danish FSA's supplementary questions. The Board of Directors and the Executive Board have stated that in practice, the head of Group Compliance & AML, who reported to the bank's CFO, was the person responsible for AML activities."

There were also obvious organisational failures that undermined the independence of risk management function particularly in the Estonian branch, making compliance with regulations "ineffective" (Danske Bank, 2018a):

> "In addition, the branch's second and third lines of defence were organised in such a way that in practice, they reported to the branch CEO and thus were not sufficiently independent."

5.9. Minimising Emergent Danger

A common feature of organisational disasters is that those who are closest to the problem "fail to call for help", which has been attributed to fears of causing unnecessary alarm, psychological denial of the danger or the assertion of the individual's invulnerability (Turner, 1976). Turner points out that individuals consistently underestimate the scale of the problems that they face because of ambiguity or disagreement about the evidence regarding the danger. He also notes that when the danger becomes impossible to ignore, rather than addressing the causes of the problem, individuals often look to shift the blame to others.

This was apparent in the Danske case, where unpalatable truths were ignored or downplayed (Danske Bank, 2018a):

> "For a long time, it was believed within Group that the high risk represented by non-resident customers in the Estonian branch was mitigated by appropriate anti-money laundering ("AML") procedures."

As an example, in 2012, in correspondence with the Danish FSA, the AML programme was referred to as "Best in Class" (Danske Bank, 2018a)—and indeed, it may well have been so in most areas of the Danske group, but clearly not in the Estonian branch, and the harsh criticism from regulators, over a significant time, showed:

"AML procedures also became subject to harsh criticism from the FSA in Estonia, and Danske Bank was met with regulatory sanctions from both the Estonian FSA in July 2015 and the Danish FSA in March 2016".

Danger was routinely minimised in Board reports and minutes (Danske Bank, 2018a):

"The head of Business Banking, who was responsible for the Estonian branch on the Executive Board, informed the Executive Board and Board of Directors of the observations made by GIA and the consultancy firm. The slides he had had prepared for the Board of Directors meetings **significantly toned down the AML issues**, but the Board of Directors and the Executive Board have stated that it should be taken into account that **the slides were neither shared nor used.** [And . . .]

According to minutes from meetings of the Board of Directors and the Board of Directors' Audit Committee as well as the Executive Board, there were **no comments of significance to his presentation nor to the more critical assessments** of AML in the Baltic countries in the audit report and reporting from Group Compliance & AML [Emphasis added]".

It appears that, despite the mounting evidence, the Board and management did not 'join the dots' and did not fully recognise the dangers they were facing (Danske Bank, 2018a):

"The bank's Board of Directors and Executive Board argue in their reply to the Danish FSA that such a simultaneous breakdown of all three lines of defence is a risk that must be considered to have **low probability from a management perspective**. [Emphasis added]"

The Board appeared to have blamed this on their workload (Danske Bank, 2018a):

"The Board of Directors and the Executive Board have stated that when assessing the Board of Directors' and the Executive Board's work and the volume of written material that the members of the two boards receive, it should be taken into consideration that the branch in Estonia accounts **for only a small part of the total business and total risks**. [Emphasis added]"

This section looked at each of Turner's 'stages' of a disaster and related the events that occurred over the decade that it took the scandal to emerge to these stages. The next section looks at the risks that emerged but were not managed properly.

6. Risks Apparent in the Danske Bank Scandal

In all large financial institutions, there are a myriad of risks that must be managed, proactively and carefully. First among these risks in banks are the full range of credit and market-related risks. However, this paper does not consider these major risks, as they were not raised in independent investigation, but rather other so-called non-financial risks.

6.1. Strategic Risks

A member of the US Federal Reserve Board, Kroszner (2008) noted that financial firms do not always recognise and manage risks to their corporate strategy:

"An effective overall corporate strategy combines a set of activities a firm plans to undertake with an adequate assessment of the risks included in those activities. Unfortunately, many firms have forgotten the second part of that definition. In other words, **there can be no real strategic management in financial services without risk management** [Emphasis added]."

As with the term 'strategy', there is no generally agreed definition of 'strategic risk' nor of Strategic Risk Management (SRM). MacLennan (2010) points out:

> "It is relatively recently that strategic risk management has emerged as a distinct concern. Recognition that isolated risk management in specific areas is inadequate and that many risks are "strategic" in their nature and impact has led to the emergence of the field."

McConnell (2016) collected a number of definitions of strategy and strategic risk. For example, for the purposes of examining banks, the US Federal Reserve and the Office of the Comptroller of the Currency (OCC) define "strategic risk" as (OCC, 2010):

> "The current and prospective impact on earnings or capital **arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes**. This risk is a function of the compatibility of an organisation's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation [Emphasis added]."

In the Danske case, the negative impact of earnings arises from the AML scandal, which involves both "adverse business decisions", "improper implementation of decisions", in particular, the acquisition of Sampo Pank.

In the early 2000s, Danske was following an aggressive strategy of "growth by acquisition", acquiring smaller banks in Northern Europe, such as Sampo. McConnell (2016) notes that growth strategies are risky, and acquisition strategies are particularly risky because of the "difficulty/inability of performing sufficient 'due diligence' on the firm being acquired".

In documenting many instances of commercial acquisitions that have failed, Rankine and Howson (2014) warn that "most acquisitions fail" to achieve their stated objectives and point out the importance of conducting good commercial due diligence. They note, however, that it is often very difficult to perform sufficient due diligence on the company being acquired not only in the cases where the board of the firm being pursued perceives the approach to be 'hostile' but, even when it is welcomed, in cases when secrecy, such as keeping the news of a potential takeover from employees, must be preserved.

In the case of Danske, it is apparent that the board and management did not do sufficient due diligence on Sampo Pank, since, as noted earlier, the Russian central bank had already warned that there was evidence of significant money laundering at the Estonian branch (Danske Bank, 2018a). Not that such a discovery should have stopped the acquisition, merely that additional work would be needed to resolve the problems that were later unearthed.

In short, while the overall growth through the acquisition strategy of acquiring smaller banks in Northern Europe may be considered somewhat successful, or at least not unsuccessful, the Danske Board did not identify nor did they manage the complete set of the risks in their strategy.

6.2. Strategic Technology Risk

While an opportunity was missed to identify AML issues when Sampo Pank was first acquired, later decisions turned that initial problem into a much bigger one. When in 2006, Danske announced the acquisition of Sampo Pank (Danske Annual, 2006), it clearly stated that:

> "Danske Bank expects to complete the integration of Sampo Bank's Finnish activities on its IT platform at Easter 2008. It has not yet been decided when to integrate the still relatively small operations in Estonia, Latvia, Lithuania and Russia."

However, in 2008, the Board stated that "on the basis of a cost analysis, the Group decided to discontinue the migration of Banking Activities Baltics to its shared IT platform." (Danske Annual, 2008). This meant that as time went on (Danske Bank, 2018a):

> "The Estonian branch had its own IT platform. This meant that the branch **was not covered by the same customer systems and transaction and risk monitoring as Danske Bank Group** headquartered in Copenhagen (also referred to as "Group"), and it also meant that Group **did not have the same insight into the branch as other parts of Group.** [Emphasis added]".

This anomaly proved a serious shortcoming for the bank's risk monitoring functions, compounded by the fact that many of the documents were written in Estonian or Russian and thus difficult for foreigners to read.

In the Danske case, the board and management had a clear strategy of 'one platform', based on shared state-of-the-art technology. However, the board chose not to follow that strategy for the Baltic branches for cost reasons. In this, they failed to fully understand and manage the risks in the overall technology strategy (McConnell, 2017)

6.3. Operational Risks

In 2004, the Basel Committee of the Bank for International Settlements, the world's senior banking regulator, finalised proposals to bring the management of Operational Risk in line with the standards already adopted for Market and Credit risks (Bank for International Settlements, 2004). These so-called Basel II proposals are designed to strengthen operational controls in international banks and to ensure that they have set aside sufficient capital to cover large losses, such as those at Danske Bank. The Basel Committee defines operational risk as (Bank for International Settlements, 2004):

> "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but not strategic or reputational risk".

In the 2004 Basel II regulations, 'Money Laundering' is identified as an Operational Risk Loss Event Type in the category of "Clients, Products & Business Practices", in the Level 2 Category "Improper Business or Market Practices" (Bank for International Settlements, 2004, Annex 7). The Danske case would seem to fit this classification, and hence, the losses are clearly an Operational Risk Loss Event (ORLE).

It is also obvious that all of the factors identified by the Basel Committee as giving rise to operational risk were present in the Danske case, including:

- Processes—failure of basic processes designed to identify money laundering;
- People—failure to follow board level policies, in particular reporting suspicious activities with regard to 'non-residents';
- Systems—failure to integrate IT systems in the Estonian branch into the 'one platform' technology model; and
- External—illegal money laundering activity by non-residents.

It is apparent from the evidence provided in the independent report (Danske Bank, 2018a) and others that, at least for management of the operational risks of money laundering, the 'Group operational risk management framework of policies' and IT systems were woefully deficient.

7. Failure of Risk Management

It should be noted that this study did not consider all aspects of risk management at Danske Bank, only those areas relating to failures of Anti-Money Laundering policies, and even then, only with regard to the firm's Estonian branch. In the absence of any other information that shows wider failures of risk management elsewhere in the firm, which has *not* emerged following the revelations in the independent report (Danske Bank, 2018a), it may be assumed for now that this scandal is an outlier, albeit a very serious one.

7.1. Operational Risk Management

In its 2008 Annual Report, as Sampo Pank was being acquired, the Danske Board reported that as regards operational risk management (ORM) (Danske Annual, 2008):

> "**Group operational risk management relies on a framework of policies**. Each individual business unit is responsible for the day-to-day monitoring of operational risk and for mitigating losses. The relevant support functions place resources at the disposal of the business units. The measurement and control framework comprises four **qualitative** elements:
>
> - Risk identification and assessment ensure that all key risks are **effectively highlighted** for group-wide transparency and management. This enables the Group to focus on fewer but more fundamental risks.
> - Monitoring of key risks is an ongoing process ensuring that **an increase in such risks is highlighted on a consistent and a group-wide basis**.
> - Risk mitigation strategies and implementation processes ensure **that key risks are reduced and establish transparency in these strategies and processes**.
> - Follow-up on loss data and events. [Emphasis added]"

In its initial 'Risk Management Report' to its Danish regulator (Danske Bank, 2010), it was noted that the "Executive Board" had a dedicated "Operational Risk Committee" which "includes managers of all major support functions and resource areas, including IT, and the Group Business Development department" and which:

> "[...] reviews trends in the Group's key operational risks on an ongoing basis and **follows up on the progress of** concrete **action plans regarding these risks**. The committee also receives reports and recommendations on key risk indicators." [And ...]
>
> The Group's operational risk losses are registered in the Operational Risk Information System (ORIS). Losses are categorised according to the Basel II event categories for operational risk, and both direct losses and direct gains are registered. [Emphasis added]"

Thus, Danske Bank appeared to have 'ticked all the boxes' as regards regulatory required policies, organisations and frameworks for operational risk management but, as noted by the independent inquiry, "all three lines of defence failed", and the much-vaunted risk management framework did not work.

7.2. Failures of Operational Risk Management

The independent investigation summarised the failures of operational risk management in the Estonian Branch (Danske Bank, 2018a):

> "In respect of the Estonian branch, **there were deficiencies in all three lines of defence**. The first line of defence at the branch **did not focus on efficiently combating money laundering despite the significant** number **of high-risk, non-resident customers**. This was not identified by the first line of defence at Business Banking in Copenhagen, which received a number of reports stating that the branch complied with the rules. **The second-line integration of the Baltic units into the Group's risk management**, including monitoring and reporting, was weak. AML at the branches in the Baltic countries was not mentioned as a compliance risk in the bank's management reporting. The third line internal audit formed part of Group Internal Audit (GIA**). The integration of the branch's internal audit department with GIA was also inadequate**. [Emphasis added]"

The core problem in this case is that, despite the many red flags raised by regulators, correspondent banks and a whistle-blower, the issue was not raised to a level that the Board and senior management would take the warnings seriously. Despite what management considered to be a world-class risk management framework, the right information did not flow to the right people (Danske Bank, 2018a):

> "Several documents show how management in Copenhagen did not integrate the Estonian branch in the bank's risk management and control systems, but instead allowed the branch to operate with significantly different risk exposure and to a large extent, the branch itself conducted controls."

Such a situation is clearly a serious failure of ORM processes in the bank, which was long-lived (over a decade) and catastrophic, causing serious economic and reputational damage to the company.

How could such a failure happen, though?

Documenting a large number of ORM failures, Blacker and McConnell (2015) identified similar operational risk management failures including in Barings, Allied Irish Bank (AIB), National Australia Bank (NAB), Société Générale (SocGen), Union Bank of Switzerland (UBS) and JPMorgan. Several of these cases are often categorised as 'rogue trading', but in all these cases, breakdowns in operational risk management processes enabled the people responsible to precipitate serious losses.

A key point about many of these cases, and also obvious in the Danske case, is the 'remote' nature of the staff and business units involved in the risk management failures. Before these scandals erupted, the offices and business units involved were considered to be small and reasonably profitable, and the small size of the business was wrongly considered not to be risky.

This, however, is a flawed analysis. Whereas the level of credit risk may reasonably be tied to business unit size, this is not true of operational risk, as failures in ORM in even a small business unit can bring about very large regulatory fines. Operational risk is no respecter of size or profitability.

7.3. Key Lesson of Danske Scandal

The key lesson of the Danske Bank scandal is that operational risk management (ORM) processes failed, not across the whole firm but, disastrously, in a small, remote business unit that was considered by HQ as hardly worth worrying about. Turner (1976) showed that once such an incorrect belief takes hold, it becomes accepted wisdom and very hard to dislodge.

In some respects, **the solution is obvious and simple**—apply the most rigorous risk management analysis and management to *every* business unit in the firm, even if, at first glance, the effort may not appear to be justified.

In terms of the Basel II regulations (Bank for International Settlements, 2004), this means that every business unit should, each year, conduct a formal and rigorous risk and control self-assessment (RCSA) exercise, in which all operational risk issues pertaining to the business unit would be documented, considered and improvements canvassed.

As a *separate and independent* exercise, this business line RCSA exercise should be reviewed and audited independently by the firm's central risk management organisation and also the internal audit function. At this stage, any whistle-blowing reports related to the business unit would be considered and used to validate the business unit's self-assessment.

The results of these reviews should then be presented to senior business line and executive risk committees for formal analysis, monitoring and sign-off. Any requests for additional information or for process changes should be formally made to business unit management and monitored during execution by the central risk management function. Additionally, in order to pick up systematic problems across business lines, formal assessments of RCSAs by independent experts should be commissioned on a regular basis.

To many business unit managers, such recommendations might appear to be bureaucratic overkill—ticking even more boxes—and to an extent, they are. However, as Turner (1976) observes and Danske Bank shows, barriers to the free flow of information down and up the organisation need to be minimised, regulations need to be respected, warnings, especially from well-positioned whistle-blowers, need to be heeded and risks must be treated seriously.

In short, boards and senior executives must endure that their risk management policies and frameworks are effective, *everywhere in the organisation.*

8. Further Research

This paper was an historical case study and so, except for references, is not compared in detail here to other significant cases of risk management failures. Additional research could prove useful by studying:

- Similarities and differences between the Danske case and other scandals in which failure of AML processes were apparent;
- Mechanisms for identifying, describing and mitigating money laundering risks that may lead to misconduct and large operational risk losses; and
- The success, or otherwise, of regulators' actions in the Danske and in other cases, identifying, if possible, factors that are likely to impact successful implementation of regulatory policies.

It should be noted that such research efforts are necessarily multi-disciplinary, for example, involving not only ORM experts but also Human Resources, Compliance and Payments functions.

Another potentially useful area of research is that of formal methodologies for studying operational risk case studies, especially those that have involved large-scale operational risk losses. Turner's method is useful because it is based on a structured approach to analysis that attempts to dig down to the root causes of an organisational disaster. Fitzsimmons and Atkins (2017) highlight some of the benefits of Turner's approach in taking a big-picture, longitudinal perspective of an event that has had major ramifications for a firm or the industry:

> "When time separates causes from effects, feedback is likely to be poor and more distorted by bias. This makes it much harder for people and organizations to learn and to identify the roots of future crises. Festering root causes can incubate and accumulate for years before emerging; so unless someone deliberately sets out to find and deal with them, they will stay that way until they materialize to cause a crisis. Even when they emerge in a crisis, these deeper risks often remain unrecognized because, . . . , the investigation is superficial and does not dig to root causes".

In this study, Turner's well-established framework is employed, and doubtless, there are others. Research to identify and compare other potentially useful methods could prove beneficial to regulators, the industry and academics.

9. Summary

This paper presents an historical case study of what has become known as the Danske Anti-Money Laundering (AML) scandal in which for more than a decade, until brought to light in 2018 by an independent report, some 7.5 million payment transactions involving around 10,000 'non-resident' customers had been handled through the bank's Estonian branch, located in Tallinn. These transactions should have been deemed 'suspicious' according to the bank's AML procedures but were not.

On receiving the extremely adverse report of the investigators, the board deemed that the gross income from these suspicious pavements totalling some EUR 0.2 billion should "be donated to an independent foundation supporting initiatives to combat international financial crime".

The events leading up to the scandal are described in this paper using Turner's 'Six Stages' Framework for analysing "organisational disasters". One of Turner's key insights is that large organisational disasters, and consequential financial and non-financial losses, emerge, or are "incubated", over a long period of time, and it is difficult for those closest to the action to see the disaster emerging.

After describing Turner's methodology, the paper then describes the background to the case and, using Turner's Framework, describes the sequence of major events that took place over more than a decade that led to the exposure of the AML scandal.

The paper concluded by identifying some of the key risks that were apparent in the evolution of the Danske scandal and some lessons that can be learned, specifically the role of risk management functions in assisting business

managers to identify and mitigate the myriad of issues that give rise to such events. The paper concluded by identifying further research that could help to identify similar cases of corporate misconduct in future.

Declaration of Interest: The author reports no conflicts of interest. The author alone is responsible for the content and writing of the paper.

Appendix A. Timeline of Events

The events listed in Table A1 are an historical timeline of the events in the Danske Bank scandal, extracted from Danske Bank (2018a) and DFSA (2018, 2019) which document the same events from a different perspective and in a different order. The table contains:

- **Date(s)**: the date or dates on, or between, which the event(s) occurred;
- **Event/Activity**: the event or activity being described, as referenced in DFSA (2018) or Danske Bank (2018a), unless noted otherwise;
- **Danske Bank Reaction/Action**: how Danske Bank management, executive and/or Board reacted (or did not react) to the event or activity;
- **Red Flag**: whether the event *should have been* noticed and actions taken;
- **Features common to Disasters**: the "features" (Turner, 1976) obvious in the bank's actions/inactions, specifically:
  - (a) Rigidities of belief;
  - (b) Decoy phenomena;
  - (c) Disregard of complaints from outsiders;
  - (d) Information difficulties and noise;
  - (e) The involvement of strangers;
  - (f) Failure to comply with discredited or out-of-date regulations;
  - (g) Minimising emergent danger.

The timeline in Table A1 emerges over a number of distinctive, but overlapping, 'Phases' as described earlier:

(1) **Strategic Euphoria**: a period of euphoria as the Nordic growth strategy was implemented (roughly 2006–2008);
(2) **Regulatory Unease**: a period during which banking regulators expressed unease about the implementation of Danske's growth strategy (roughly 2009–2013);
(3) **Management Myopia**: a period during which management appeared to ignore the increasing signs of problems with the growth strategy (roughly 2013–2014);
(4) **Management Tinkering**: a period during which management took steps to ameliorate (some of) the symptoms without really addressing the serious problems emerging (roughly 2014–2016);
(5) **Management Investigations**: a period during which management initiated multiple investigations but did not directly address the problems (roughly 2016–2017);
(6) **Scandal Emerges**: a period during which the full import of the scandal emerged and corrective actions began to be taken (roughly 2017–2018); and
(7) **Aftermath**: a period during which the firm and its regulators began to take actions to attempt to correct the problems that arose during the scandal, also called "Cultural Adjustment" by Turner (1976).

Date(s)	**Event/Activity** *DFSA (2018, 2019), Danske Bank (2018a) Unless Noted*	Danske Bank—Reaction/Action	Red Flag	Turner—Features Common to Disasters
2006–2008	**Phase 1—Strategic Euphoria**			
Nov. 2006	Danske Bank acquires Sampo Pank, acquisition completed February 2007	Strategic acquisition "integration of Sampo Pank into Danske Bank's IT platform and organisation" (Danske Annual, 2006)		
2007	Estonian FSA conducted AML inspection	"not aware of the extent to which the conclusions of these reports have reached management in Copenhagen"	**Yes**	(c) Disregard of complaints from outsiders
2007	"The Russian central bank warned the Danish FSA about AML risks related to a number of Russian customers in Danske Bank's newly acquired Estonian subsidiary." (DFSA, 2019)	"The feedback received from both [heads of Legal and Audit] was that there were no problems in relation to AML risks in the Estonian subsidiary." (DFSA, 2019)	**Yes**	(c) Disregard of complaints from outsiders (e) The involvement of strangers
2007	"the EFSA found deficiencies in relation to the subsidiary's management of AML risks and on that basis issued an order for the subsidiary on further measures to investigate new non-Baltic customers (non-resident customers) and to strengthen internal AML procedures" (DFSA, 2019)	"However, neither Danske Bank nor the EFSA identified problems on a scale anywhere near what was later identified." (DFSA, 2019)	**Yes**	(c) Disregard of complaints from outsiders (e) The involvement of strangers (f) Failure to comply with discredited or out-of-date regulations
2008	Sampo Pank Estonia turned into Danske branch			
2009–2013	**Phase 2—Regulatory Unease**			
2009	Estonian FSA conducted AML inspections	"EFSA also concluded that EFSA had found some weaknesses, but did not find serious shortcomings or problems, and that the problems identified in 2007 appeared to have been handled." (DFSA, 2019 https://www.dfsa.dk/en/News/Press-releases/2019/Corresspondance_EFSA_200219)	**Yes**	(c) Disregard of complaints from outsiders (d) Information difficulties and noise (g) Minimising emergent danger
2011–2013	Majority of new "non-resident" customers are accepted by Estonian branch	Failure to identify AML risks		(f) Failure to comply with discredited or out-of-date regulations
2012	Danish FSA's inspection	"Danske Bank has historically not lived up to its obligations in the AML area"	**Yes**	(f) Failure to comply with discredited or out-of-date regulations

Table A1 *Cont.*

Date(s)	**Event/Activity** *DFSA (2018, 2019), Danske Bank (2018a) Unless Noted*	Danske Bank—Reaction/Action	Red Flag	Turner—Features Common to Disasters
2012–2013	Estonian FSA contacted the Danish FSA about **possible AML issues** at the branch	"detailed information from 2012 and 2013 to the Danish FSA and the Estonian FSA therefore was misleading"	**Yes**	(d) Information difficulties and noise
2012–2013	"From the end of 2012 to November 2013, Danske Bank **did not have a person responsible for AML activities** as required by the Danish Anti-Money Laundering Act."	Failure to hire senior staff, as required by law	**Yes**	(f) Failure to comply with discredited or out-of-date regulations
2013	"the EFSA contacted the Danish FSA again regarding AML risks in the Estonian branch. The inquiry was based on a warning from the Russian central bank which included a list with a number of the branch's Russian customers, which the Russian central bank considered to be suspicious, and on the EFSA's own analysis of the branch's customer mix."	"The Danish FSA asked Danske Bank to address EFSA's request. The bank's acting Head of the Legal Department replied that the Estonian branch had a special setup in the light of the elevated AML risk in the branch." (DFSA, 2019)	**Yes**	(c) Disregard of complaints from outsiders (f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
May 2013	New Group Credit Policy removing exception "to grant FX lines to non-residents solely on cash collateral", i.e., to end 'non-resident' accounts	Assumption that Group Policy would be implemented as dictated		(a) Rigidities of belief
July 2013	"following a dialogue with the bank, one of the Estonian branch's two correspondent banks for USD payments **terminated its cooperation with the branch due to concerns about the branch's non-resident customers**"	Failure to recognise significance of this event	**Yes**	(c) Disregard of complaints from outsiders
2010–2013	"The Danish FSA requested additional detailed documentation, depending on the quality of the information, and compared it with the information from the EFSA's AML supervision of the branch, [. . . .] Thus, the Danish FSA did not uncritically trust the information from the bank—neither information on AML in the branch in Estonia or on the Danish activities." (DFSA, 2019)	"However, the evidence shows that the bank did not always provide the FSA with accurate information, and that in several cases this was due to the bank not being sufficiently thorough in its investigation of the facts before replying to the Danish FSA." (DFSA, 2019)	**Yes**	c) Disregard of complaints from outsiders (d) Information difficulties and noise (f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
Sept. 2013	New CEO (Thomas Borgen) appointed, previously Head of Baltic Banking, including Estonian branch			
2013–2014	**Phase 3—Management Myopia**			
Dec. 2013	"senior employees at the bank **received a whistle-blower report** about AML issues in relation to a customer in the Estonian branch's non-resident portfolio"	Failure to recognise significance of the whistle-blower's report	**Yes**	(f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
End 2013	Accounting Goodwill for Estonian branch written down			(g) Minimising emergent danger

Table A1 *Cont.*

Date(s)	**Event/Activity** *DFSA (2018, 2019), Danske Bank (2018a) Unless Noted*	Danske Bank—Reaction/Action	Red Flag	Turner—Features Common to Disasters
March 2014	GIA (Group Internal Audit) reported that new Group Credit Policy **has not been fully implemented**	Failure to react to process failure	**Yes**	(f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
Jan 2014	The whistle-blower made additional accusations in relation to **three other customers of the branch**	Failure to react to warnings	**Yes**	(g) Minimising emergent danger
Feb. 2014	GIA "confirmed significant AML deficiencies as pointed out by the whistleblower"	Failure to react to warnings	**Yes**	(g) Minimising emergent danger
April 2014	"an investigation by an external third party. . . . . identified 14 critical deviations and 9 significant deviations between branch practice and applicable rules/best practice"	Failure to react to warnings	**Yes**	(f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
May 2014	In an investigation of "a general nature". "There was thus significant information from the whistleblower that the person responsible for AML activities or others **failed to follow up on or did not sufficiently follow up on**"	Failure to react to whistle-blower's information	**Yes**	(c) Disregard of complaints from outsiders (g) Minimising emergent danger
May 2014	"At the request of the bank's CEO, the person responsible for AML activities in May 2014 prepared a plan to give the AML area a lift at the Baltic units. . . . . The **plan and the branch's own review did not solve the significant problems at the branch**."	Failure to act on agreed changes	**Yes**	(f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
2014–2016	**Phase 4—Management Tinkering**			
2014	"the EFSA conducted two AML inspections in 2014. The Danish FSA was not asked to attend. The inspections showed significant weaknesses in the branch's AML procedures and led to orders from the EFSA and the replacement of the branch's local management." (DFSA, 2019)			(c) Disregard of complaints from outsiders (f) Failure to comply with discredited or out-of-date regulations
June 2014	"At a new audit found a number of customers who "should not have been accepted as continuing customers of the branch"	Failure to implement Group Credit Policy	**Yes**	(f) Failure to comply with discredited or out-of-date regulations
End 2014	"According to the bank's Board of Directors and Executive Board, the branch's review, completed towards the end of 2014, led to the termination of 853 customer relationships"	Failure to expedite termination policy		(d) Information difficulties and noise

Table A1 *Cont.*

Date(s)	**Event/Activity** ***DFSA (2018, 2019), Danske Bank (2018a)*** ***Unless Noted***	Danske Bank—Reaction/Action	Red Flag	Turner—Features Common to Disasters
Mid 2014	"the Estonian FSA conducted AML inspections at the branch and **was very critical in its reporting**"	Failure to react to warnings "the Estonian FSA's **critical conclusions were thus still toned down in** the minuted discussions of the Executive Board and in written internal reporting to the Board of Directors."	**Yes**	(c) Disregard of complaints from outsiders (g) Minimising emergent danger
Aug. 2014	Russian Laundromat exposed (OCCRP, 2014)	Failure to recognise implications of reporting	**Yes**	(e) The involvement of strangers (g) Minimising emergent danger
Sept. 2014	"a senior employee sent an e-mail to other senior employees at Group Legal and Group Compliance & AML ... "The executive summary of the Estonian FSA letter **is brutal to say the least and is close to the worst I have ever read within the AML/CTF area** (and I have read some harsh letters)."	Failure to react to internal warnings "According to [omitted], there **was no cause for panic as the findings have been addressed in the ongoing process improvement**. [Omitted] will travel to Estonia and assist the Estonian organisation."	**Yes**	(a) Rigidities of belief (c) Disregard of complaints from outsiders (g) Minimising emergent danger
Oct. 2014	"In the bank's annual AML report for the period from October 2013 to September 2014, Group Compliance & AML **underlined the AML challenges faced by the** bank, for example in Estonia"	Failure to react to warnings	**Yes**	(f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
Jan. 2015	"the Board of Directors **did not make a decision**, but noted the Executive Board's **expected close down** of the part of the non-resident portfolio ... "	Failure to follow-up implementation "**Another year passed before**, in January 2016, the close down was completed"		(a) Rigidities of belief (g) Minimising emergent danger
May 2015	"one of the branch's **two correspondent banks informed the bank that it no longer wanted to assist in transactions** with British companies controlled by the branch's Russian customers"	Failure to react to warnings	**Yes**	(c) Disregard of complaints from outsiders (g) Minimising emergent danger
July 2015	Estonian FSA 'harshly' criticised AML procedures	Continued running down Non-Resident Portfolio	**Yes**	(f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
2015	Non-Resident Portfolio terminated	Finally closed early 2016		
Sept. 2015	"The **other of the two correspondent banks terminated its cooperation** with the branch in ... due to concerns over the branch's non-resident customers"	Failure to react to warnings	**Yes**	(c) Disregard of complaints from outsiders (g) Minimising emergent danger

Table A1 *Cont.*

Date(s)	**Event/Activity** *DFSA (2018, 2019), Danske Bank (2018a) Unless Noted*	Danske Bank—Reaction/Action	Red Flag	Turner—Features Common to Disasters
2016–2017	**Phase 5—Management Investigations**			
Jan. 2016	"the close down [of non-resident portfolio] was completed . . . as a result [inter alia] of pressure from the Estonian FSA"			
April 2016	At the hearing on the Panama Papers in the Danish Parliament's Fiscal Affairs Committee in April 2016, the bank's preliminary investigations **had uncovered only seven customers with companies registered by the Panamanian law firm Mossack Fonseca**"	"**The bank later had to state that the Estonian branch had had more than ten times as many customers with companies established by Mossack Fonseca.**"	**Yes**	(a) Rigidities of belief (d) Information difficulties and noise (e) The involvement of strangers (g) Minimising emergent danger
April 2016	Danske Bank publicly announced that the bank would scale down its Baltic banking activities, focusing "exclusively on supporting subsidiaries of Nordic customers and global corporates with a significant Nordic footprint"			
March 2017	Reporting of the Russian Laundromat, in the Danish media	Failure to react to warnings	**Yes**	(a) Rigidities of belief (c) Disregard of complaints from outsiders (d) Information difficulties and noise (e) The involvement of strangers (g) Minimising emergent danger
April 2017	"the bank hired [external party] to investigate why the bank's controls had failed."	"However, **the investigation did not cover the extent of suspicious transactions** and customer relations"		(a) Rigidities of belief (d) Information difficulties and noise (e) The involvement of strangers
Sept. 2017	"A [Danish FSA] inspection was begun following stories in the media about the Azerbaijani case in September 2017"			
Sept. 2017	"As a result of the media coverage of the Azerbaijani case . . . the Danish FSA asked the bank's Board of Directors and Executive Board **for a written statement about this case and more generally about AML handling at the branch**"	"The Danish FSA received a statement from the bank on 16 October 2017."	**Yes**	(c) Disregard of complaints from outsiders (d) Information difficulties and noise (e) The involvement of strangers (f) Failure to comply with discredited or out-of-date regulations
2017–2018	**Phase 6—Scandal Emerges**			
Sept. 2017	Danske Bank acknowledged that it was "major deficiencies in controls and governance that made it possible to use Danske Bank's branch in Estonia for criminal activities such as money laundering" (Danske Bank, 2017)	Not all information shared 'for legal reasons' related to regulators	**Yes**	(d) Information difficulties and noise (f) Failure to comply with discredited or out-of-date regulations

Table A1 *Cont.*

Date(s)	**Event/Activity** *DFSA (2018, 2019), Danske Bank (2018a) Unless Noted*	Danske Bank—Reaction/Action	Red Flag	Turner—Features Common to Disasters
Sept. 2017	"The bank did not initiate an investigation into the transactions until September 2017"	Failure to react to warnings		(f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
Oct 2017	"During 2017, the bank has several times provided information or material about the case to the Danish FSA.	"As a result of **inadequate information being provided to the Danish FSA**, the Danish FSA has found it necessary to **enquire more than once regarding the same issues** in order to receive an adequate reply and to enquire about the bank's knowledge of further cases."	**Yes**	(c) Disregard of complaints from outsiders (d) Information difficulties and noise (f) Failure to comply with discredited or out-of-date regulations
Oct. 2017	Danske Bank has been placed under investigation by French Authorities	Subsequently, investigation changed the status of Danske Bank to that of an assisted witness.	**Yes**	(c) Disregard of complaints from outsiders (f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
Nov. 2017	"not until November 2017 [did the bank] initiate an investigation into the course of events and into whether managers or staff had sufficiently lived up to their responsibilities"	Failure to react to warnings	**Yes**	(a) Rigidities of belief (f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger
Dec. 2017	"the bank hired a law firm to handle and supervise the investigations."			
Dec. 2017	"the Danish FSA sent a memorandum entitled "Preliminary assessments of the involvement of Danske Bank's management in the AML case at the bank's Estonian branch to Danske Bank"		**Yes**	(f) Failure to comply with discredited or out-of-date regulations
Feb. 2018	"The Chief Audit Executive replied on 6 February 2018, and the Board of Directors and the Executive Board replied on 7 February 2018. The reply from the Board of Directors and the Executive Board **included more than 200 pages of annexes**"	" . . . **the bank's investigations of what had happened in the AML area in Estonia were in the initial stages and that the replies to specific questions therefore necessarily were incomplete**"	**Yes**	(a) Rigidities of belief (d) Information difficulties and noise (e) The involvement of strangers (f) Failure to comply with discredited or out-of-date regulations (g) Minimising emergent danger

Table A1 *Cont.*

Date(s)	**Event/Activity** ***DFSA (2018, 2019), Danske Bank (2018a) Unless Noted***	Danske Bank—Reaction/Action	Red Flag	Turner—Features Common to Disasters
March 2018	"The Danish FSA received a reply with a number of general comments on 26 March 2018. The reply from the Board of Directors and the Executive Board also included more than 600 pages of annexes"	"Danske Bank has **chosen to let the law firm handling the bank's investigations represent the Board of Directors in the case in relation to the Danish FSA**."	**Yes**	(a) Rigidities of belief (c) Disregard of complaints from outsiders (d) Information difficulties and noise (g) Minimising emergent danger
April 2018	"The process [of answering questions] has thus been rather long"		**Yes**	(f) Failure to comply with discredited or out-of-date regulations
May 2018	Publication of Danish FSA "Danske Bank's management and governance in relation to the AML case at the Estonian branch"	"Danske Bank earlier concluded that, in the period from 2007 to 2015, **it was not sufficiently effective in preventing the branch in Estonia from potentially being used for money laundering** and that this was due to critical deficiencies in governance and controls."	**Yes**	
Sept. 2018	Publication of Danske internal "Report on the Non-Resident Portfolio at Danske Bank's Estonian branch" (Danske Bank, 2018a)	"According to assessments made, the Board of Directors, the Chairman and the CEO **have not breached their legal obligations** towards the bank"	**Yes**	(a) Rigidities of belief (c) Disregard of complaints from outsiders
Sept. 2018	CEO (Thomas Borgen) resigns			
2019– . . .	**Phase 7—Aftermath**			
Feb. 2019	Estonian FSA orders Danske Bank to close Estonian branch			
Feb. 2019	Danske Bank in dialogue with US securities industry regulator (SEC)			
Oct. 2019	Danske Bank closes Estonian branch (Reuters, 2019)			

Table A1 Timeline of significant events in the Danske Bank scandal.

References

Augustine, N. R. (1995). Managing the Crisis you tried to Prevent. *Harvard Business Review*, *73*(6), 147–158.

Bank for International Settlements. (2004). *International Convergence of Capital Measurement and Capital Standards—A Revised Framework*. Basel: Bank for International Settlements, Basel Committee on Banking Supervision. Retrieved from http://www.bis.org/.

Blacker, K., & McConnell, P. J. *People Risk Management*. London: Kogan Page.

Danske Annual. (2006). *Annual Report 2006*. Copenhagen: Danske Bank. Retrieved from https://danskebank.com/.

Danske Annual. (2007). *Annual Report 2007*. Copenhagen: Danske Bank. Retrieved from https://danskebank.com/.

Danske Annual. (2008). *Annual Report 2008*. Copenhagen: Danske Bank. Retrieved from https://danskebank.com/.

Danske Annual. (2018). *Annual Report 2018*. Copenhagen: Danske Bank. Retrieved from https://danskebank.com/.

Danske Bank. (2010). *Risk Management Report 2010*. Copenhagen: Danske Bank. Retrieved from https://danskebank.com/.

Danske Bank. (2017, September 21). *Danske Bank Expands Investigation of Estonia Branch*. Copenhagen: Danske Bank. Retrieved from https://danskebank.com/.

Danske Bank. (2018a, September 19). *Report on the Non-Resident Portfolio at Danske Bank's Estonian Branch*. Copenhagen: Danske Bank. Retrieved from https://danskebank.com/.

Danske Bank. (2018b). *Interim Report—First Nine Months 2018*. Copenhagen: Danske Bank. Retrieved from https://danskebank.com/.

Danske Bank. (2018c, September 19). *Conference Call Findings of the Estonia Investigations*. Copenhagen: Danske Bank. Retrieved from https://danskebank.com/.

Danske Bank. (2018d, October 1). *Danske Bank Appoints Interim CEO*. Copenhagen: Danske Bank. Retrieved from https://danskebank.com/.

DFSA. (2018, May 3). *Danske Bank's Management and Governance in Relation to the AML Case at the Estonian Branch*. Copenhagen: Danish Financial Supervisory Authority. Retrieved from https://www.dfsa.dk/.

DFSA. (2019, January 29). *Report on the Danish FSA's Supervision of Danske Bank as Regards the Estonia Case*. Copenhagen: Danish Financial Supervisory Authority. Retrieved from https://www.dfsa.dk/.

Fitzsimmons, A., & Atkins, D. (2017). *Rethinking Reputational Risk: How to Manage the Risks That Can Ruin Your Business, Your Reputation and You*. London: Kogan Page.

Gleick, J. (1992). *Genius: Richard Feynman and Modern Physics*. Abacus.

Hofstede, G. (1991). *Cultures and Organizations*. London: McGraw-Hill.

Kroszner, R. (2008, October). *Strategic Risk Management in an Interconnected World*; Washington: Federal Reserve Board. http://www.federalreserve.gov/newsevents/speech/kroszner20081020a.htm.

MacLennan, A. (2010). *Strategy Execution: Translating Strategy into Action in Complex Organizations*. T & F Books UK.

McAndrews, D. H. (2010). Payments Systems. In A. N. Berger, P. Molyneux & J. O. S. Wilson (Eds.), *The Oxford Handbook of Banking. Oxford Handbooks in Finance*. Oxford University Press. Kindle Edition.

McConnell, P. J., & Blacker, K. (2011). The role of Systemic People Risk in the Global Financial Crisis. *Journal of Operational Risk*, *6*(3), 65–123. [CrossRef]

McConnell, P. J. (2003). *AIB/Allfirst—Development of another Disaster*. Henley Working Paper Series; Henley Management College.

McConnell, P. J. (2005). *NAB—Learning from Disaster*. Henley Working Paper Series; Henley Management College.

McConnell, P. J. (2010). Prime Loss: A Case Study in Operational Risk. *Journal of Risk Management in Financial Institutions*, *3*(1), 84–104.

McConnell, P. J. (2013). Strategic Risk—The Beanstalk Syndrome. *Journal of Risk Management in Financial Institutions*, *6*(3), 229–252.

McConnell, P. J. (2014). Dissecting the JPMorgan Whale: A post-mortem. *Journal of Operational Risk*, *9*(2), 59–100. [CrossRef]

McConnell, P. J. (2015). *Systemic Operational Risk*. London: Risk Books.

McConnell, P. J. (2016). *Strategic Risk Management*. London: Risk Books.

McConnell, P. J. (2017). *Strategic Technology Risk*. London: Risk Books.

Nyberg, L. (2011, March). *Misjudging Risk: Causes of the Systemic Banking Crisis in Ireland*; Dublin: Ministry of Finance. Retrieved from http://www.bankinginquiry.gov.ie/Documents/Misjuding%20Risk%20-%20Causes%20of%20the%20Systemic%20Banking%20Crisis%20in%20Ireland.pdf.

OCC. (2010). *Large Bank Supervision—Comptrollers Handbook*; Washington, DC: Office of the Comptroller of the Currency. Retrieved from https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/large-bank-supervision/index-large-bank-supervision.html.

OCCRP. (2014). The Russian Laundromat. Organized Crime and Corruption Reporting Project. Retrieved from https://www.occrp.org/en/laundromat/russian-laundromat/.

OCCRP. (2017). The Russian Laundromat Exposed. Organized Crime and Corruption Reporting Project. Retrieved from https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/.

OCCRP. (2018). Russia Laundered Millions via Danske Bank Estonia. Organized Crime and Corruption Reporting Project. Retrieved from https://www.occrp.org/en/investigations/7698-report-russia-laundered-billions-via-danske-bank-estonia.

Rankine, D., & Howson, P. (2014). *Acquisition Essentials: A Step-by-Step Guide to Smarter Deals* (2nd ed.). London: Pearson Educational.

Reuters. (2019, October 1). Danske Bank Has Exited Its Banking Activities in Estonia. Retrieved from https://www.reuters.com/article/brief-danske-bank-has-exited-its-banking/brief-danske-bank-has-exited-its-banking-activities-in-estonia-idUSC7N1V001S.

Turner, B. (1976). The Organisational and Interorganisational Development of Disasters. *Administrative Science Quarterly*, *21*, 387–397. [CrossRef]