Discussion Paper of the State of Anti-Money Laundering

Prof Tom Kirchmaier
(with input from Jan Damsgaard, Jonas Hedman and Kalle Johannes Rose)
CCG, CBS
04 May 2023

Summary

With Denmark's Financial Services Industry having now caught up with the international level of anti-money laundering (AML) (and other) compliance standards, it is time to look at the system in a holistic manner and ask questions about efficiency, effectiveness and costs. Compliance is important, as it ensures a clean financial system and provides efficient support to the police in the fight against organised crime, amongst others.

The argument we are making in this short note is that the global AML compliance system does little to deter money laundering activity by professional actors. Currently, we are spending too much time on the 'small' fish, and not the 'large' ones. However, the system imposes substantial costs on banks, and hence society at large (a back-of-the-envelope calculation puts the annual costs for compliance in banks operating in Denmark at just under USD 1 billion pa).

As we have been arguing for some time, the system will need to be redesigned so that it is sufficiently risk-based, with large parts of it being automated. This will both bring down the costs and make better use of compliance staff to focus on risk-based investigations.

We are making a number of recommendations on technical automation below, but one important pre-condition will be that both the law and financial regulators' guidelines, are harmonised across the Nordic countries (and beyond).

Preamble

Following the Danske Bank money laundering scandal – and similar problems at Nordea, Swedbank and others – there was general consternation that this could have happened in a well-functioning country like Denmark. The generally high level of trust within Danish society made it a low priority, probably coupled with a lack of understanding that money laundering (ML) is a global phenomenon that pays little respect to local norms. Having made the necessary investments into processes and people, it is now time to think of how to lift the system up to the next level to be much better, faster and cheaper. Denmark – and its generally high level of digitisation – can in principle provide the ideal sandbox for innovation in the AML field, should the institutions allow it. As happens so often, a crisis can catapult a country from a laggard to a leader in an area, provided it makes the right choices.

Size of the Issue, and its Origin

ML occurs when the sources of funds need to be disguised for one reason or another. This means that, to define effective defences against it, we will need to have a proper understanding or taxonomy of the demand for ML services. No one clearly understands how big the problem really is, but estimates of the size of the illegal economy range from 1% to 5% of a given GDP. With the global GDP reaching about USD 100 trillion, the amounts that need to be 'washed' globally and every year range from USD 1 trillion to USD 5 trillion. Whatever the true number, it is a substantial amount, putting serious pressure on all AML systems around the world. The demand for these ML services

will be originating from organised crime groups operating professionally worldwide. Their main income stream will be from the drug trade, but many of their other income sources will be at least as harmful (if not more) for society: illegal drug trade, illegal weapons trade, human slavery, child sexual exploitation, racketeering and fraud, environmental crime and lately cybercrime.

There will be additional sources of funds that are not the direct proceeds of traditional criminal activity, namely the embezzlement of state funds, tax evasion, currency control and serious corruption, often originating in countries with weak institutions. The amounts will be in addition to the ones mentioned above[1]. There is also the issue of countering terrorist financing (CTF) which was bolted onto the AML system following the 9/11 attacks in the United States. But unlike some of the political backers of this CTF initiative, we have our doubts that financial institutions are the right ones to stop it, and argue that better endowing the police service might give society a much better return – but more about that later.

People often ask about how big the issue is in relation to the Danish banks, or the Nordic banks more generally, and the honest answer is that nobody fully knows. To give some indication though, the latest Danish National Risk Assessment on Money Laundering cites the UN calculus which puts it at about DKK 68bn annually[2]. But given the constant pressure on the system, defining the potential volume is almost irrelevant, as we know that ML professionals will make use of the opportunity the minute the defences are lowered (as they did in the past).

To summarise, the issue we are facing is that every year there are trillions of US dollars (or the equivalent in other respective currencies) that need to be turned into legitimate funds so that they can be of use to their beneficiaries. And given the size of the constant capital stream, this also means that there will be constant pressure on all of the defences globally, and like water, ML constantly searches for the weakest link.

Efficiency and Effectiveness of the Current System

One way to assess the effectiveness of our AML defences is to look at the market price for professional money laundering services. Clearly, there is not an open market for these kinds of services, and there exists a large spectrum in terms of volumes that are dealt with. However, we do know from various European police (and other) sources that for very large amounts, the market price is somewhere in the 8% range (or less). Obviously, the price for smaller amounts does go up, but often does not exceed 20%. This means that after deducting the costs (bribes, etc.) of the activity, the implied detection likelihood is close to zero. But we think what we will have to accept is both that the market is very efficient and that the professionals do not fear being detected. We do, however, 'pick up' people in the process. However, many of those could be labelled small and/or inexperienced and are probably those who will not cause much harm to society (and hence who we are not really interested in).

We do, however, observe that the process imposes substantial costs on the customers in the form of much higher transaction costs (opening accounts, moving larger amounts or providing proof of income/costs). It also imposes substantial costs on the banks in the form of much higher compliance costs for AML and otherwise. In Appendix A, we summarise some rough back-of-the-envelope

[1] Moreover, there will be problematic sources of capital that result from avoidance of currency controls, but this is more of an issue in Asia as large volumes of capital are trying to leave China.
[2] DEN NATIONALE RISIKOVURDERING AF HVIDVASK (2022); p. 15.

calculations that puts the annual costs for compliance work for banks with business in Denmark slightly below USD 1 billion annually. In our opinion, this is a remarkable amount, and probably not in relation to the harm that is caused by those we are likely to detect (small or inexperienced, as mentioned above).

We are not arguing that we should reduce our focus on disrupting suspicious transactions. But we do argue that as a society (globally) we will have to develop solutions that are much better, cheaper, and faster (efficient and effective). One step in this direction will be to gain a better understanding of the demand side, in other words, those criminals who make use of ML services. Another is to use the data we have much better, improve our empirical models in many ways and share data (which, we believe, can be done without violating existing legal requirements).

Our over-arching objective must be to design a financial system that is on the one hand very efficient, but on the other hand does not allow itself to be abused by dubious actors to launder money from criminal or other illegal or problematic sources.

Banks as an Extension of the Police Service?

Before we delve into the technical details of better detection models, we wanted to pick up a thought to which we referred earlier, when talking about terrorist financing.

Starting with decisions by the G7, and followed by international agreements and standards co-ordinated through the FATF (Financial Action Task Force) in Paris, politicians globally have given all banks a substantial role in law enforcement by making them follow the money and detect suspicious payment activities. However, this is yet to be supported by giving the banks the wide-ranging responsibilities needed to do the job effectively. Not giving them wide-ranging powers is clearly the right thing to do, as we do not want bankers to be police officers. But, on the other hand, that also makes them inefficient regarding some of their tasks, as they do not have access to the same data, tools, and rights/powers as law enforcement agencies.

Hence, at times and for specific tasks (e.g., terrorist financing), it might be more sensible to better endow the police service and potentially finance it with a levy on the banks (that is smaller than the compliance costs for that specific task). The simple idea is that the returns to public security might be higher when spending on the police than on banks. Obviously, the police will then be responsible for any and all of their activities, even if financed through a bank levy.

NEXT STEPS

Harmonise Legislation Across the Nordics?

The first recommendation we make is of a non-technical nature: to harmonise legislation and enforcement of compliance across the Nordics. This work should be streamlined and one should undertake a greater Nordic …, where the various systems and laws are standardised.

Historically, each country has its own legal framework that is guided by European Union (EU) regulation. In the latest EU AML Directive, individual member countries have less room for interpretation, which will naturally force a certain standardisation. Having said that, the aim should be to develop texts as identical to one another as possible, not least as we will also want to achieve a standardisation of the rulebook and actions of the various financial regulators, together with private public (and academic) partnerships (PPPs), tax authorities across the Nordics. In the long run this can

serve as a blueprint for a wider European cooperation framework. This has several important advantages:

- Banks that operate across the Nordics typically operate with one rulebook, which means that they might be (close to) breaching the rules in one country or another. This also means that certain activities might need to be expensively duplicated across the various countries.
- It will allow for the standardisation of processes and IT systems, which could even lead to centralisation of certain activities across borders.
- Equally, given the small size of the countries, the knowledge pool of people who intimately know the national legislation, and can either write rules or advise on them, is very limited. Standardising the legislation would allow for the substantial widening of the knowledge pool, improving the debate and therewith also the quality of advice that can be given.

Improve Data Sharing

In Appendix C we discuss extensively the legal aspects of sharing relevant AML data across banks in Denmark. We conclude that we see no reason why this should not be done for the effective assessment of transactions (and customers). Here the Danish Banking data centres like Bankdata, BEC or SDC would be a practical place to start, but as we have said, this could and should be standardised and automated.

How to Improve Detection?

As discussed, the issue we are facing is that the public (via banking service fees) invests a substantial amount of money into detecting illicit payments and rogue actors, while probably having little impact on the activities on the ground (measured by market prices).

This occurs because the current empirical approach to detection lacks an 'outcome variable'. Hence, we cannot run a regression or a machine learning model without a fundamentally different approach (which we suggest below). The industry helps itself by relying on so-called 'scenarios', which are essentially accidentally observed past instances of ML. These scenarios are also very finite in number (typically <130) and are probably known to the 'other side' as well. In any case, they are of limited effectiveness. We should also keep in mind that larger banks have much more resources, and with it likely to have higher standards than some of the (many) smaller banks in Denmark in respect to ML processes.

Having said that, there are in our opinion many ways to make a step change regarding the effectiveness of the detection algorithms, if only we allow experimentation with different approaches.

The key will be to switch our detection from individual observations (for which we will naturally run against the limits of privacy and GDPR laws) to aggregation by small areas. For this, we drop all personally identifiable information and replace it with an area indicator of where that private person lives, or in the case of business, where they operate.

This aggregation into small areas works very well, and in the past, it has allowed us to build the reference model for crime prediction for the United Kingdom. These small areas work so well because people self-select into homogenous groups in terms of where they choose to live (you are very similar to your neighbour(s)). This in turn allows us to understand the socio-economic structure, preferences and wealth position of any area – everything we need to know for a good prediction

model. And given that the information is now free from privacy concerns, we have a format that allows us to share data amongst banks and between the authorities and the banks. This might also be a way to take the very important work of the Danish JIMLIT initiative to the next level and help to automate it.

The Nordics, being one of the most digitally savvy and organised societies, would provide a prefect laboratory for experimentation in this area. They have been trendsetters in terms of many digital innovations, and it would be natural if they lead in this area too. We believe that the payoffs to society would be enormous.

The Central Role of the Regulator

To succeed with any innovation initiative in this area, the buy-in of the banking regulator(s) is key. Banks will not innovate beyond the clear guiderails set by the regulator, as they want to avoid being reprimanded. On the other hand, banking regulators typically have little appetite to push innovation, and there are many reasons for this, not least as the regulator operates within the limits of the law and other regulations, which typically leave little room for experimentation. Moreover, the law passed by the Danish parliament on the Danish Financial Supervisory Authority (DFSA) sandbox does not allow enough room for the sandbox to be used for this purpose (AML testing). Hence, we are stuck in a negative steady state between a risk-adverse administration, banks that will merely comply with the regulation and an industry that sells over-priced solutions but delivers only limited change on the ground.

In summary, if we are keen to improve the efficiency and effectiveness of AML procedures within banks, we need to think how we can empower – and even instruct – the regulator to systematically allow for experimentation within banks. For this, we would also need to ensure equal access to such – let's call it Sandbox 2.0 – and to a certain degree, potentially even exempt banks from certain risks they take in the process for a limited period of time.

Pre-clearance, Federated Systems and Digital Currencies (CBDCs)

In the mid-term, an alternative would be to pre-clear actors and give them as well as their transactions a clean bill of health ex-ante. Good guides are the so-called federated systems – and we discuss the AML application of it in detail in Appendix B – where we trust the decision of another bank about the nature of a transaction or customer. This could be easily implemented in the above-mentioned banking data centres and will save the participant banks substantial amounts of money as they can stop duplicating activities. There is the question of liability, but in practice the risk in well-functioning systems will be small. Moreover, we need to keep in mind that in a risk-based system, errors are unavoidable (they also occur currently, but in the new system we will be open about this), and in the short run any potential fines and losses can be covered by the savings from avoiding duplication. Such a system will also require a good feedback loop, which will be easy to implement. Such a system could then be transposed to Central Bank-issued Digital Currencies (CBDCs, like the e-crown or e-EURO) if and when there are issues.

Appendix A: *What Danish Banks Spend on Compliance and AML*

In the following, we try to estimate the likely annual costs of 'Compliance and AML' by banks in Denmark (i.e., the Danish operation of both local and international banks). We base our analysis on the figures from Danske Bank, as it is the only bank that publishes such figures as part of their accounts. This naturally means that we are exposed to a number of biases, which luckily go in the opposite direction and will, in part, cancel each other out. On the one hand, it is likely that Danske Bank might invest more than the others in this particular area at the moment, in part to correct historical shortcomings. Hence, to base it only on Danske's figures will mean we are likely to overestimate the total amount spent in Denmark. On the other hand, we lack the necessary accounting data for some smaller banks (36 in total), hence excluding them for our analysis. This means that we will underestimate the total amount.

In any case, the purpose of this exercise is to provide a rough estimate of the likely expenditure on 'Compliance and AML', and not to provide a point estimate. So how did we arrive at our rough range?

Data

The accounting data used for these calculations has been drawn from Orbis. Orbis categorises financial institutions by different consolidation codes, which are as follows:

- C1: statement of a mother bank integrating the statement of its controlled subsidiaries or branches with no unconsolidated companion
- C2: statement of a mother bank integrating the statements of its controlled subsidiaries or branches with an unconsolidated companion
- C*: additional consolidated statement
- U1: statement not integrating the statements of the possible controlled subsidiaries or branches of the concerned bank with no consolidated companion
- U2: statement not integrating the statements of the possible controlled subsidiaries or branches of the concerned bank with a consolidated companion
- U*: additional unconsolidated statement

For this analysis, we have chosen to use the consolidation codes C1, C2 and U1, since we are interested in the aggregated bank spending.

The variables we have drawn for the period 2017–2020 are:

- Number of employees
- Total assets in USD
- Deposits and short-term funding in USD

The data for 2021 was still incomplete at the times of our analysis, and hence are not included here.

As we mentioned above, Orbis does not carry the accounting data for some smaller banks, nor does any other dataset we have access to. Thus, at this point we can only acknowledge this omission, which stands as follows:

Year	2017	2018	2019	2020	2021
Number of banks in our dataset	79	82	79	75	71
Total number of organisations holding a banking license	100	96	95	90	89

Table 1: The actual number of Danish banks compared to the number of banks on which we draw from the database. This includes both Danish banks and branches of foreign banks. The actual number of banks in Denmark is taken from FinansDanmark: https://finansdanmark.dk/tal-og-data/institutter-filialer-ansatte/

So, we see that the issue will probably be bigger than what these calculations can account for.

The Estimation

	2017	2018	2019	2020	2021
USD	284,354,499	388,173,981	710,920,847	898,994,895	823,092,383
DKK	1,875,404,082	2,452,260,012	4,742,021,203	5,874,278,071	5,178,693,147

Table 2: The Danish banks' AML and compliance spend calculated based on the figures from Danske Bank, with the yearly currency exchange from Denmark's Nationalbanken: https://nationalbanken.statbank.dk/nbf/100249.

Appendix B: Federated Risk-Based Anti-Money Laundering System

AML is a centralised task that every bank runs. For instance, the payer's and the payee's banks check the same transaction, which is part of banks' obligations if they are to remain compliant. In a federated system, actors trust each other, since each actor fulfils its obligations, including risk assessments, Know Your Customer (KYC) and transaction monitoring. An illustration of how a federated risk-based system works is airport security. Copenhagen airport does not need to check all transferring passengers that arrive from Berlin because Copenhagen trusts that Berlin has done a thorough security check. Hence, there is no reason for Copenhagen Airport to repeat this process.

Another example is WAYF (Where Are You From), which allows someone with credentials, for instance, from a Nordic university, authority or public institution, to log into each other's systems. For example, if Aarhus university trusts students and Copenhagen Business School (CBS) trusts Aarhus University, then CBS can admit Aarhus students into its systems without running any security risk. One system using WAYF principles is EDUROAM, which allows academics and students who are trusted at one institution to log into all other participating academic institutions' Wi-Fi systems.

Let us provide an illustration of how a federated risk-based AML system could work in terms of payments. Many transactions are local Business-to-Business or Business-to-Consumer, and frequently involve transactions between each other. So, if bank A trusts bank B, who in turn trust its customer X, then that trust can be transferred via credentials to bank A. When customer X makes a transaction with any of Bank A's customers, neither Bank A nor B needs to check the transaction. Note that a federated system is already in place at the central bank level.

This part of an AML system would focus on mitigating unwanted transactions that harm society. A federated risk-based AML system can do this. This type of system must manage two levels. The first level comprises the financial actors, today indirectly (criminal party using an existing customer of a financial actor) and directly (criminals are clients of a financial actor) used as ML service providers. The second level is the transactions where some will be unwanted. A distributed risk-based AML system should include the following key elements:

1. Intra-bank risk assessment: The bank should conduct a thorough risk assessment to identify and evaluate potential money laundering risks across different business lines, products, services and geographic locations and score them (1 = no risk, 5 = very risky).
2. Know Your Customer (KYC): The bank has typically already implemented robust and transparent (for other banks) KYC procedures to gather information on customers and their transactions, and assessed the level of money laundering risk associated with their transactions and scored them (1 = no risk, 5 = very risky).
3. Transaction monitoring: The bank should continuously monitor transactions to detect and flag any suspicious activity, for instance change in transaction patterns, and score them (1 = no risk, 5 = very risky).
4. Reporting and investigation: The bank should be able to report suspicious activity to the relevant authorities and conduct investigations as required.
5. Feedback: Relevant authorities and banks must disclose transaction credentials.

Elements 1–3 are key for creating transaction credentials. It is the transaction, not the costumer, who is in focus in a federated transaction monitoring system.

Appendix C: Data Sharing and Anti-Money Laundering Regulation

From the incorporation of the 4th AML Directive (4AMLD) in the EU, much emphasis has been placed on the significant impact that data sharing amongst financial institutions could have on the prevention of ML. However, the approach to data sharing in Denmark has remained somewhat cautious. An explanation for this can be found if we look at the individual actors and their mutual interaction. In terms of the financial institutions, the sanctioning level of breaching privacy regulation (no matter if it is GDPR or the Charter of Fundamental Rights) is quite high. Because the regulatory boundaries between AML regulation and GDPR is unclear, the behaviour of the financial institutions can be explained by the simple fear of sanctioning by the regulator. There is, furthermore, disagreement on whether the banks – due to bank secrecy rules – can share information about customers with each other, if the balance between the AML regulation and GDPR should permit this.

On the other hand, the competent authorities in Denmark have also had a very reactive stand towards data-sharing. The behaviour of the competent authorities in Denmark can partly be explained by the ambiguity of the EU regulation in itself, which until the recent ECJ ruling of 22 November 2022 has not been clear in legal terms. However, the explanation also has to be found in a general lack of competences or understanding of risk-based regulation. If the competent authorities had a comprehensive understanding of the risk-based approach to regulation, they would have been able to address data sharing in a proactive manner, simply because the ambiguity between privacy regulation and AML regulation is caused by the risk-based approach. Consequently, the reactive approach from the national competent authorities has enhanced the fear of sanctioning in the private sector, decreasing the incentive to share data.

The regulatory ambiguity – or conundrum – between privacy regulations, bank secrecy rules and AML regulations is caused by the risk-based approach to regulation, which is new, especially in civil law countries. A recent ruling by the European Court of Justice (ECJ) specifies the boundaries between privacy and AML regulation and clarifies that in general, data governed by privacy regulations (such as GDPR) can only be breached if there is a legitimate reason to do so.[3] Such a legitimate reason is given by the AML regulation if there is a present risk of money laundering. The rationale being that privacy is protected unless crime is apparent. Following this risk-based principle, data sharing should be possible in two circumstances:

1. Where risk of money laundering is apparent,
2. Where data does not include information protected by GDPR or the Charter of Fundamental Rights.

In terms of data sharing, particularly two approaches have been discussed but hindered by the reactive approach due to regulatory ambiguity: sharing risk scores of customers and sharing generic data to compare AML methodology. In terms of the first approach, a sharing of risk scores should by no means be understood as a sharing of privacy-protected data, since the risk score merely represents the financial institutions' own perception and evaluation of the available information and inherent risks. Thereby, there should by default not be any hindrance to sharing such data. In the second case, the sharing of generic data would bring enormous benefits to society and facilitate the aligning of the method and evaluation of money laundering risk across financial institutions, whereafter a divergence in comparison could serve as a red flag indicator of either the client or the method. If the contained data does not include private information, the sharing of models and data

[3] ECJ C-37/20 of 22 November, 2022.

in favour of conducting a better approach to the prevention of money laundering should not be considered in breach of GDPR nor the Charter of Fundamental Rights. There are however still a number of uncertainties concerning the interaction between bank secrecy rules in the Financial Business Act.