
Report by Finance Denmark's Anti-Money Laundering Task Force

Anti-money laundering and counter-terrorist financing in the Danish financial sector

CONTENTS

page 04 Indledning	page 06 Recommendation summary	page 10 Money laundering and terrorist financing – who, what and how much?	page 18 Banks' current response
page 27 Challenges relating to an- ti-money laundering and counter-terrorist financing	page 28 Dilemmas	page 36 Recommendations of the Anti-Money Laundering Task Force	page 37 Main track 1: Joint IT solutions
page 47 Main track 2: Stronger partnerships with authorities	page 55 Main track 3: Training	page 60 Main track 4: Principles of conduct	page 64 Main track 5: Increased transparency
page 68 Appendices			

FOREWORD

Cases of financial crime relating to money laundering and terrorist financing have dominated newspaper headlines and news broadcasts in recent years. With good reason. Against this background, it has been necessary for financial institutions, authorities and society at large to take action.

At the annual meeting of Finance Denmark in 2018, the financial sector made a collective commitment to solve the set task of being among the best in the world to detect and combat money laundering and other fraud, making it possible to clamp down on the forces that misuse banks for criminal purposes. The individual financial institutions are striving every day to achieve that ambition. On the back of these individual efforts, Finance Denmark was mandated to initiate targeted joint efforts to combat financial crime, including to set up an Anti-Money Laundering Task Force (the "Task Force") consisting of financial sector representatives and four external experts. The Task Force has now been working for 11 months, and the result is this report including sector recommendations to combat financial crime going forward. The recommendations should be seen as a supplement to the initiatives already launched by banks individually and together, and to the political initiatives launched by the Danish Parliament and the EU by way of AML packages and generally increased regulation. To the Task Force, replacing silo mentality with collaboration and providing banks with tools to meet their corporate responsibility in relation to anti-money laundering and counter-terrorist financing were key.

Combatting financial crime will be a top priority on the financial sector's agenda in the years to come. The Task Force's recommendations will take us one step further in the fight against financial crime. And with these constructive initiatives involving specific recommendations for the sector and the authorities, including new joint IT solutions, a new confidential intelligence unit, new principles of conduct, improved training and increased transparency, we believe the scene is set for an even stronger commitment across the sector and society at large.

With these recommendations, the sector aims to lead the way – and we look forward to a continued constructive dialogue about the recommendations to combat money laundering and terrorist financing.

Enjoy the read!

Linda Nielsen, Chairman of the Anti-Money Laundering Task Force, and Michael Rasmussen, Chairman of Finance Denmark.

INTRODUCTION

Mandate of the Task Force

In the wake of a string of money laundering cases, Finance Denmark has set up a task force charged with exploring and recommending ways to strengthen the fight against money laundering and terrorist financing through joint and industry-wide initiatives and solutions going forward.

Together with banks' own initiatives, these recommendations will form the basis for closer partnerships with the authorities and ensure clear, coordinated and consistent communication about challenges and solutions. The financial sector must, in every context, demonstrate that it makes a serious and concerted effort to ensure that all possible steps are taken to enhance awareness, quality and efficiency in all parts of the sector.

Four main tracks

The work of the Task Force will be divided into four main tracks.

1. Joint IT solutions

The Task Force will be exploring the possibilities of wider collaboration on joint IT solutions to enhance the quality and effectiveness of measures taken to combat money laundering and terrorist financing. The scope for an industry-wide solution for the onboarding of customers – personal as well as business customers – will be analysed. Efforts along the same lines are required in connection with the establishment of the statutory centralised bank account register, and the Task Force will be contributing ideas and solutions of mutual benefit to society, the authorities and the sector. The joint solutions must take into consideration regulation in the fields of competition and data protection law.

2. Stronger partnerships with authorities

The Task Force will look into the possibilities of strengthening partnerships with the authorities.

Meetings are held already with the Danish Financial Supervisory Authority (FSA), the State Prosecutor for

Serious Economic and International Crime, the Danish Security and Intelligence Service, the Danish Ministry of Industry, Business and Financial Affairs and other authorities, both under the auspices of Finance Denmark and bilaterally between the major banks and the authorities. It will be determined how partnerships with the authorities can best be optimised, including which initiatives may specifically be launched to enable the sector and the authorities to unite in an effective and concerted effort to combat money laundering and terrorist financing. In that connection, the Task Force will, together with the authorities, look to other countries for inspiration, such as the UK and the Netherlands. Especially the UK has a very successful Joint Money Laundering Intelligence Taskforce (JMLIT).

3. Self-regulation and ethics

The Task Force will be exploring the conditions for, experience from and scope for applying self-regulation and ethical guidelines. Experience from, for instance, Sweden's and the Netherlands' use of guidelines and industry codes of conduct will serve as inspiration.

4. Certificering

The Task Force can also look into the possibilities of creating a common framework for anti-money laundering certification of staff in Danish banks.

The Task Force is also mandated to address other themes that it considers to be relevant.

The work will be completed by Q4/2019 when the recommendations will be submitted to the Board of Directors of Finance Denmark. Finance Denmark's Task Force consists of representatives from the Danish banks as well as four external experts. In addition, Finance Denmark has provided secretariat services to the Task Force.

¹ Det vil senere fremgå af rapporten, at Hvidvask Task Forcen har ønsket et spor om øget transparens i sektoren. Dette vil udgøre hovedspor 5 i rapporten.

Members of Finance Denmark's Anti-Money Laundering Task Force

External experts

- Chairman: Linda Nielsen, Professor, Faculty of Law, University of Copenhagen
- Lars Krull, Senior Advisor, Aalborg University
- Per Gunslev, State-Authorised Public Accountant and former Partner, EY
- Anne Birgitte Gammeljord, Attorney, Rovsing & Gammeljord

Internal sector representatives

- Carsten Egeriis, Chief Risk Officer, Danske Bank
- Anders Jensen, Group Managing Director, Nykredit
- Anita Nedergaard, Country AML Responsible, Nordea Denmark
- Bo. A. Christensen, Managing Director of Business Service, Jyske Bank
- Lene Lorentzen, AML Officer, Sydbank
- Karin Duerlund, Head of Legal, Spar Nord
- Anders Balle Rasmussen, Area Director, Sparekassen Kronjylland
- George Wenning, Head of Section, Legal, LOPI

Secretariat

- Ulrik Nødgaard, Managing Director, Finance Denmark
- Kjeld Gosvig-Jensen, Executive Director Legal, Finance Denmark
- Stine Luise Goll, Executive Director Communications, Finance Denmark
- Jens Kasper Rasmussen, Senior Adviser, Finance Denmark
- Cecilie Sander Bernbom, Senior Consultant, Finance Denmark
- Camilla Thorning, Head of Press, Finance Denmark

RECOMMENDATION SUMMARY

25 specific proposals for anti-money laundering and counter-terrorist financing measures - the social contract calls for societal tools

Over the past 10 months, the Task Force has identified, analysed and discussed the role and contribution of the financial sector in relation to anti-money laundering (AML) and counter-terrorist financing (CTF). The work has been centred around four tracks laid down in the Task Force's mandate and a supplementary track (increased transparency) as requested by the Task Force.

The result of this in-depth work is 25 specific recommendations to banks, Finance Denmark, authorities and society at large. The aim of the Task Force has been to ensure that banks commit more strongly to the social contract, meeting society's reasonable expectation that the financial sector will lead the way. In this context, it has been essential to the Task Force also to provide recommendations on how the financial sector obtains the tools and resources necessary to solve this task – also from the authorities. Broadly speaking, a defined social obligation calls for specific societal tools.

The 25 recommendations address many areas and impose obligations on the sector, trade organisations, authorities and society at large. The majority of the recommendations are solutions for implementation in the financial sector and Finance Denmark. The most extensive recommendations include: a vision for industry-wide IT collaboration by 2025, a joint AML/CTF intelligence unit, six principles of conduct, training collaboration and experience sharing, raising awareness of the general public, an annual conference and report describing the scope and efforts, safe-deposit box monitoring, whistle-blower support, in-depth evaluation of reported money laundering suspicions, a collaboration with the Danish Financial Intelligence Unit (the Money Laundering Secretariat under the State Prosecutor for Serious Economic and International Crime), and increased focus on EU cooperation.

For a brief description of the 25 recommendations, see below:

Main track 1: Joint IT solutions

1. Five specific anti-money laundering IT projects

- The Task Force recommends wider collaboration on joint IT solutions to combat money laundering – and wider efforts to combat financial crime
- Against this background, the Task Force recommends the implementation of five specific AML IT projects:
 1. KYC [Know Your Customer]: New common customer due diligence standard
 2. Passport validation: New solution to validate matches between civil registration [CPR] and passport numbers
 3. Joint PEP/RCA register: New joint register to be operated by the authorities
 4. Joint data register: Register of the above three initiatives
 5. Account ownership portal: Portal showing who holds a bank account or safe-deposit box.

2. Vision for industry-wide IT collaboration by 2025

- The Task Force recommends the immediate launch of a pre-project to identify precisely what is required to realise the vision for industry-wide IT collaboration by 2025. The aim of long-term, comprehensive, industry-wide AML/CTF collaboration is very ambitious, and many technical and regulatory challenges will have to be overcome in the process. For instance, legislative changes will be required for banks to be able to share customer data.
- The Task Force recommends investigating, on the basis of this pre-project identification, whether a shared industry utility can be set up to streamline the collection, verification, storing and sharing of data and documents supporting the sector's AML/CTF procedures and processes. The purpose would be to combat and prevent money laundering and terrorist financing using digital and data-driven solutions.
- The Task Force recommends that the vision for industry-wide IT collaboration be linked closely to the recommendation of stronger partnerships with authorities, including the Joint AML/CTF Intelligence Unit [recommendation no 4].

Main track 2: Stronger partnerships with authorities

3. Dilemmas must be exposed

- The Task Force recommends that the sector and public authorities jointly discuss the dilemmas relating to AML/CTF measures, based on considerations taking into account the nature of information and the nature of the crime, and look at how to optimise collaboration in general, including the general exchange of information, and the possibilities of exchanging information in concrete cases.

4. Danish JMLIT equivalent: Joint AML/CTF Intelligence Unit

- The Task Force recommends that a Joint AML/CTF Intelligence Unit be set up with representatives from banks, the police, the Danish Defence Intelligence Service, the Danish Security and Intelligence Service and the Danish Tax Agency.
- The Task Force recommends the introduction of a separate provision in the Danish AML Act allowing the authorities, within the framework of the General Data Protection Regulation and the Danish Financial Business Act, to set up this unit, which will provide a forum for exchanging confidential information on "big fish" and cases with major social impact subject to appropriate precautionary measures.

5. AML Forum

- The Task Force recommends that the Danish AML Forum should not only support the sharing of knowledge and experience but should also work to ensure a truly holistic approach across authorities in the form of, for instance, common supervisory priorities.

6. Danish Data Protection Agency

- The Task Force recommends that the Danish Data Protection Agency play a larger role in the AML Forum and the AML Forum+.

7. Digitaliseringsstyrelsen og Udbetaling Danmark

- Task Forcen anbefaler, at det overvejes, om Digitaliseringsstyrelsen og Udbetaling Danmark skal inddrages i HvidvaskForum og HvidvaskForum+.

8. Quarterly report and feedback from the Danish Financial Intelligence Unit on suspicions reported

- The Task Force recommends that the Danish Financial Intelligence Unit (FIU) look at ways to improve feedback on reports made by the financial sector to the authorities.

Main track 3: Training

9. Case-based training and experience sharing

- The Task Force recommends that AML officers be offered training programmes that include experience sharing, case work and dilemmas.

10. Biannual conferences focusing on experience sharing

- The Task Force recommends that Finance Denmark hold biannual conferences with experience-sharing opportunities. This will promote uniform behaviour across the sector in practice.

Main track 4: Principles of conduct

11. Six principles of conduct

- The Task Force recommends six principles of conduct to the sector, supporting its anti-money laundering and counter-terrorist financing commitment.

12. Focus on culture and transparency

- The Task Force recommends that the sector, building on the principles of conduct, focus on ethics before profit, that the need for oversight be recognised and that a targeted development of the corporate culture be pursued.

13. Tone from the top, cascading down the organisation

- The Task Force recommends that the sector, building on the principles of conduct, focus on setting the tone from the top and that all parts of an organisation underline the importance of combating money laundering and terrorist financing.

Main track 5: Increased transparency

14. Management commentary

- The Task Force recommends that the individual banks undertake to outline their anti-money laundering and counter-terrorist financing commitment, including their AML policy, in the management commentary of their annual reports.

15. Dedicated webpage

- The Task Force recommends that on their websites, the banks dedicate a webpage to providing targeted and publicly available information about their anti-money laundering and counter-terrorist financing commitment.

16. Annual conference

- The Task Force recommends that Finance Denmark hold an annual conference thematising some of the challenges and dilemmas relating to financial crime.

17. Annual report

- The Task Force recommends that Finance Denmark prepare an annual report with a detailed account of the sector's efforts in the area, including the development in reports made, allocation of resources, staff etc.

18. Raising awareness

- The Task Force recommends that Finance Denmark increase its efforts to raise awareness among bank customers and the general public, explaining banks' efforts in this area and their obligations, including in relation to the collection of customer data and the purpose of this. This could be done through information campaigns, social media, pamphlets and direct (e)mail to bank customers.

Further initiatives

19. Whistle-blower support

- The Task Force recommends that the respective boards of directors – in addition to ensuring whistle-blower schemes in all banks – consider how to support whistle-blowers, for example by offering legal advice..

20. Collaboration with the State Prosecutor for Serious Economic and International Crime

- The Task Force recommends that the sector, by way of the Joint AML/CTF Intelligence Unit, allocate staff to an exchange programme focusing on knowledge sharing for a period of up to three months.

21. Evaluation of reports to the Danish Financial Intelligence Unit

- The Task Force recommends that the sector, together with the Danish FIU, annually evaluate the

reports made by banks to assure that they are of appropriate quality for the purpose of investigating suspicious activity and to avoid unnecessary reporting.

22. Safe-deposit boxes

- The Task Force recommends that the sector compile data on safe-deposit boxes. The reason for focusing on safe-deposit boxes is that they may be used to store criminal property, drugs, black money, etc.
- The Task Force then recommends that the sector consider more closely how to establish a satisfactory level of preventive measures and processes when banks offer this service.
- The Task Force furthermore recommends that the sector enter into a dialogue with the Danish FSA on industry guidelines with respect to effective monitoring of safe-deposit boxes as part of customer due diligence and monitoring requirements.

23. Banking Forum under AML Forum+

- The Task Force recommends as a supplementary political initiative that, in addition to the AML Forum for authorities and the AML Forum+ for authorities and trade organisations, a Banking Forum focusing

on banks be set up with representatives from Finance Denmark and its members. Such a forum would provide a platform for detailed and industry-specific mutual knowledge sharing as well as discussions about specific topics.

24. EU+

- The Task Force recommends that Finance Denmark work to ensure that future EU regulation include a specific option for member states to establish bodies similar to the Danish Joint AML/CTF Intelligence Unit and for cross-border exchange of information between these national units.

25. Guidelines on the Danish AML Act

- The Task Force recommends a continued focus on providing up-to-date guidelines on the anti-money laundering legislation, supporting in particular those areas where AML and other legislation conflict, as well as guidance on specific situations where legislative history provides little guidance.



MONEY LAUNDERING AND TERRORIST FINANCING

– WHO, WHAT AND HOW MUCH?

Money laundering as a concept is used in many contexts and was even named word of the year 2018 in Denmark. Terrorist financing has not received the same amount of mention, but it is a focus area of at least the same importance. But what do the concepts cover, and who are the criminals? The definitions are important in order to understand the scope of efforts required to eliminate money laundering, terrorist financing and consequently financial crime and how big and resource-intensive the task actually is.

Who are the financial criminals?

Do the financial criminals launder money through banks – or do banks launder money for the criminals? Is there a difference? You sometimes wonder when reading in the press about the money laundering scandals.

Overall, it is important to understand that money laundering and terrorist financing can be committed by both little and big fish. As regards money laundering, not only professional criminals such as drug cartels, terrorists and IT fraudsters attempt to launder illegal funds. Money launderers can also be little fish, such as local builders who deposit income from undeclared work or pensioners who commit social fraud to receive higher supplementary pension benefits. Money laundering

and terrorist financing are currently penalised under the Danish Criminal Code.

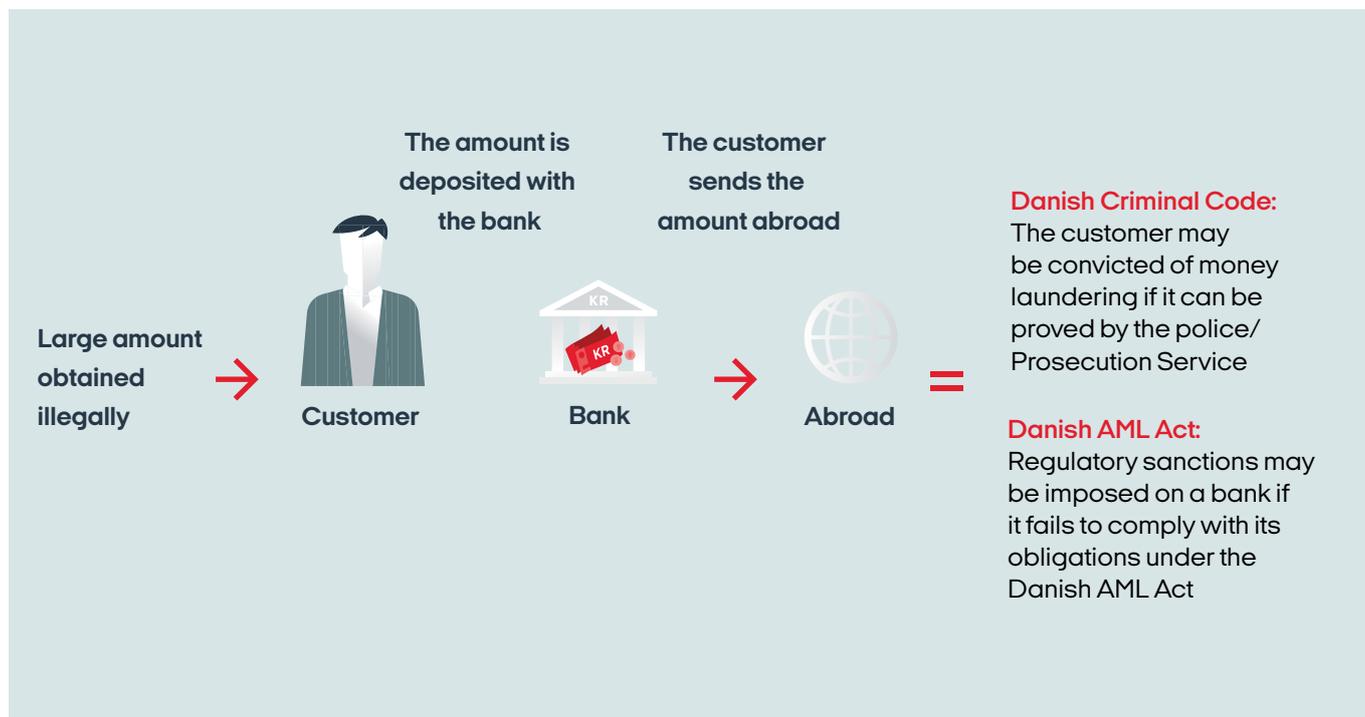
The role of banks

So what is the role of banks? Banks are part of society's gatekeepers in the sense that they must primarily seek to spot, and notify the authorities of, customers who intend to launder money or contribute to terrorist financing, and they must also, through monitoring and follow-up, investigate whether customers are attempting to launder money or finance terrorists. In other words, banks are guarding the gates to the financial system.

That is not a simple task. To perform these duties, banks must comply with a series of requirements laid down in the Danish Act on Measures to Prevent Money Laundering and Financing of Terrorism [Danish AML Act]. They include rules to ensure that the sector has adequate measures to prevent and combat money laundering and terrorist financing. For instance, the Act stipulates that banks must prepare a risk assessment of their business based on authority input and own experience. Against that background, banks must prepare policies and business procedures, and AML/CTF measures must be part of their customer relationship management, transaction execution etc.

²Kilde: Straffelovens §§ 290 og 290 a og § 114 b

Figure 1 Case: Distinction between the Danish Criminal Code and the Danish AML Act



Source: sections 290, 290 a and 114 b of the Danish Criminal Code.

Banks are thus required to identify any suspicious behaviour or activity, investigate whether the suspicion can be disproved, and if not, report it to the Danish FIU and in some cases stop the transaction.

As a final aspect of the role of banks, money laundering transactions in the financial sector are sometimes allowed to proceed for the benefit of the overall efforts to combat financial crime. Authorities can ask a bank to keep a customer after a suspicion has been reported, for instance to avoid compromising an investigation of other larger cases or to obtain evidence to prosecute the criminals. Banks can also assist the authorities in other ways, and they can disseminate warnings and other knowledge to customers to raise their awareness, helping to prevent financial crime and thereby enhancing society's overall defence.

Distinguishing between breaches of the Danish Criminal Code and of the Danish AML Act

Money laundering and terrorist financing are subject to penalty under the Danish Criminal Code. Persons guilty of money laundering or terrorist financing are not penalised under the Danish AML Act but under the Danish Criminal Code. This is an important difference, as actual money laundering or terrorist financing requires criminal intent as well as an active, punishable act. If a bank is aware that funds derive from criminal activities or are intended to finance terrorism and still assists with transactions without notifying the authorities, the bank (and any related persons conducting the acts with the same knowledge and intent) will be liable to punishment for complicity under the Danish Criminal Code.

The Danish AML Act, on the other hand, focuses on the duty to have strong AML/CTF measures. The Act does not criminalise the intent to commit money laundering or terrorist financing, or complicity; this falls within the scope of the Danish Criminal Code.

Also, breach of the Danish AML Act does not depend on money laundering or terrorist financing actually being committed. Rather, it depends on a discretionary assessment of whether a business subject to the Act, e.g. a bank, has adequate measures to prevent it from being used for money laundering or terrorist financing purposes; if not, it does not fulfil its obligations. Therefore, if a bank does not comply with the requirements of risk assessment, monitoring etc of the Danish AML Act, the bank is not deemed to have laundered money, but it may have created a possibility for customers to use the bank for their own criminal purposes.

The challenge of preventing criminals from exploiting the financial system exists in, for instance, the initial contact between a bank and its customers and in the bank's subsequent monitoring of customers. Banks must reject a customer if the customer's identity cannot be established and verified. But a customer committing financial crime is not always a criminal to begin with. Broadly

speaking, customers rarely enter the bank looking like one of Duckburg's Beagle Boys.

If a customer [financial criminal] requests a banking relationship involving products that correspond to those sought by a comparable customer, and the customer is generally cooperative and presents a financial position and transaction pattern as can be expected for that type of customer, the bank will typically not be able to detect the customer's criminal intent. At a later point, when the customer's behaviour is evidently unusual and suspicious, the bank will already have been exploited for the customer's criminal activities. Against its every intention.

Money laundering

The concept of money laundering is broad and covers, for instance, the act of unlawfully obtaining, receiving or storing financial proceeds to which you are not entitled. The money laundering concept in anti-money laundering legislation also includes tax evasion, and as there is no minimum amount, it also includes social fraud and undeclared work, as mentioned above.

The Danish AML Act defines money laundering as follows:

1. To unlawfully receive or obtain for oneself or others a share in profits or means obtained through criminal offence
2. To unlawfully conceal, store, transport, assist in the disposal of or otherwise subsequently serve to secure the profits or means obtained through criminal offence
3. Attempts at or participation in such actions
4. Arrangements made by anyone who committed the offence from which the profits or means stem.

Money laundering occurs, for instance, when illegal funds are placed in the financial system and their origin is disguised through transactions. That way, the funds can be separated from their original source and may subsequently appear to be legitimate. An example is if black money mixed with legitimate "white" money is deposited into a bank account and subsequently transferred to several foreign accounts, or if an object of high value is purchased using black money and subsequently sold, making the profit appear to be legitimate.

Figure 2 Money laundering in practice

	Exampel A	Exampel B	Exampel C
<p>Placement</p> <p>The illegal proceeds are placed, for instance through the financial system.</p>	<p>Depositing cash with a bank (possibly blended with proceeds from legal activities).</p>	<p>Taking cash abroad.</p>	<p>Using cash to purchase high-value goods, real estate or assets for business purposes.</p>
<p>Layering</p> <p>The illegal proceeds are disassociated from their source, for instance through (financial) transactions.</p>	<p>Electronic transfer to foreign accounts (often using companies with no real activity, or the funds are disguised as proceeds from legal activities).</p>	<p>Depositing cash with a bank abroad.</p>	<p>Selling the goods/ assets purchased.</p>
<p>Integration</p> <p>The illegal proceeds are returned to the money launderer, for instance in a form where they have been converted into funds or assets that appear legitimate.</p>	<p>Return of funds as payment of (fictitious) loans or (fictitious) invoices.</p>	<p>A complex network of national and international transfers, making it almost impossible to identify the origin of the funds.</p>	<p>Income from real estate or activities appearing to be legitimate</p>

Source: Danish Prosecution Service.³ (This is Finance Denmark's own translation)



The main purpose of the very extensive anti-money laundering framework is to help combat very serious crime, including human trafficking, drug-related crime, terrorism etc [big fish], at global level. This is the background to the very strict and far-reaching rules in eg the US and the EU. However, money laundering also comprises other types of financial crime [little fish]. One example is undeclared work, which implies failure to pay the tax

Section 114 b of the Danish Criminal Code defines terrorist financing as acts committed by any person who:

1. directly or indirectly provides financial support to
2. directly or indirectly procures or collects means to; or
3. directly or indirectly places money, other assets or financial or other similar means at the disposal of a person, a group or an association which commits or intends to commit acts as set out in section 114 or 114 a.

due on income from services. Another example is social fraud, which implies using a bank to move around funds so the formal conditions of receiving social benefits relating to, for instance, net worth appear to be met even though this is factually not the case.

In other words, money laundering can be done in many ways and for many purposes. It is important to emphasise that it usually does not involve the use of cash. Financial criminals – especially the tough “big fish” – develop many and complex methods of misusing both the financial system and other sectors. The more fine-meshed the systems become, the keener the criminals become in their eternal pursuit of loopholes. It is a constant offensive and a difficult race, and it is imperative that collective efforts are made to continuously develop and update AML/CTF systems at all levels in order to close any loopholes that can be misused for criminal purposes.

Terrorist financing

The concept of terrorist financing is defined in section 114 b of the Danish Criminal Code.

In other words, terrorist financing is when you collect funds for, provide financial support to or make funds available to persons or groups involved in terrorist activities. Terrorist financing may be difficult to detect, as it typically involves small payments or transfers.

Also, terrorist financing is often more difficult to monitor and detect than money laundering because the “visible” illegal act is sometimes only committed after the financial system has been involved, and it is therefore the criminal intent behind the act that must be detected.

Banks may be used for terrorist financing, for instance if a customer receives legitimate income from employment or public benefits in the customer’s account, but intends to pass on amounts to persons involved in terrorist activities. Or a person raises small consumer loans that appear to be legitimate, but the funds are not used for the purposes stated and the loans are not repaid. Moreover, terrorist financing can be disguised as fundraising for charitable purposes outside the EU where the donors do not know that the money is actually used to finance terrorist activities.

What is the scope?

There are no official data on the amounts being laundered in Denmark or the scale of terrorist financing. This

means that the extent of these activities is very difficult to determine, which is also mentioned in the National Risk Assessment 2018 by the State Prosecutor for Serious Economic and International Crime.

In the Financial Action Task Force’s (FATF) evaluation report on Denmark from 2017, the scale of money laundering in Denmark is estimated at EUR 2.8 billion a year. The FATF is an inter-governmental body that promotes international AML/CTF standards. The number includes proceeds from drug trafficking, human trafficking, car theft, robberies, arms trade, smuggling of tobacco and alcohol, VAT and other tax fraud, and other financial crime. It is presumed that VAT and other tax fraud generates the largest proceeds. According to the report, the Danish authorities estimate that revenue of EUR 0.4 billion is lost every year on account of tax fraud alone. Furthermore, it is assessed that terrorist financing is primarily intended to support terrorist groups and networks abroad, but the scope is unknown.

However, despite the lack of concrete data on the scope of these activities, the implications for society of money laundering and terrorist financing are considered to be serious.

I The National Risk Assessment by the State Prosecutor for Serious Economic and International Crime emphasises the following consequences of money laundering that are detrimental to society⁴:

- The laundering of criminal proceeds nourishes, and contributes to growth in, criminal markets across the EU.
- The efforts of criminals to disguise proceeds from criminal activities may reduce confidence in the financial system.
- It may be detrimental to other related financial institutions, legislators and ordinary customers of the institution.
- It may also offend the public’s sense of justice if money laundering is perceived to go undetected or unpunished.
- It is detrimental to the economy when criminals launder proceeds from criminal activities. The consequences are direct as well as indirect, the direct consequences being in the form of a loss of tax revenue. Indirect consequences include cases where substantial proceeds from criminal activities are placed in specific types of goods or services. This may have negative implications for the markets, as it will distort competition to the detriment of persons and businesses trading legally in these goods and services. The same applies to industries characterised by a considerable “black” economy, such as certain parts of the service sector.

⁴ Source: <https://bit.ly/2s1eBTC>



Regulation

As described above, the key regulatory instrument setting out banks' obligations in this area is the Danish AML Act. The Danish AML Act is not a Danish invention but largely implements EU anti-money laundering regulation.

The EU's main regulation in the area is the so-called Anti-Money Laundering Directives, which are predominantly based on the FATF recommendations. Also, there are the sanctions lists adopted by the EU on the basis of, for instance, the UN Security Council resolutions.

The First Anti-Money Laundering Directive was adopted in 1991, imposing obligations on banks. This Directive was subsequently replaced by new EU regulation, and the latest Anti-Money Laundering Directive, the Fifth Directive, must be implemented by January 2020. The EU regulation represents a risk-based approach to

combating money laundering and terrorist financing. This means that the relevant businesses and authorities must concentrate their efforts in the areas involving the highest risk of money laundering and terrorist financing.

The Directives impose obligations on businesses, including banks, to carry out customer due diligence, monitor transactions and report suspicious activities to the authorities. In Denmark, these obligations are implemented by the Danish AML Act.

The Danish regulation also includes obligations that do not derive directly from EU regulation. Based on recent developments and money laundering cases, the political ambition has been to make Denmark leading in the EU in terms of AML regulation. A number of political agreements have therefore been concluded on national initiatives, which have been implemented by way of the Danish AML Act and other acts.

The contents of the agreements are described in detail in Appendix 2: Timeline. Below is a timeline of these political initiatives. The overview illustrates that regulation has intensified over the past couple of years.

Contents of political agreements

The political agreements from 2017 to 2019 have led to, for instance, a national anti-money laundering strategy, larger fines, increased resources to the Danish FSA and the Danish FIU, stricter fit and proper requirements, increased protection of whistle-blowers etc.

Figure 3 Timeline of selected political initiatives in the area

			National anti-money laundering strategy	
			Fifth Anti-Money Laundering Directive	
			Political agreement on enhanced measures	
		Political agreement on enhanced measures	Guidelines on Danish AML Act	Political agreement on enhanced measures
Fourth Anti-Money Laundering Directive		New Danish AML Act	Amendment of Danish AML Act	Amendment of Danish AML Act
2015	2016	2017	2018	2019

Source: Finance Denmark



BANKS' CURRENT RESPONSE

Banks play a key role in the fight against money laundering and terrorist financing in Denmark. In fact, banks are one of the most important partners to the authorities and are indisputably those who report most suspicions to the Danish FIU. This is only possible thanks to the sector's heavy investments in resources and development of IT systems in this area over the past few years. The foundation for combatting money laundering and terrorist financing is the immense legislation in this area. Legislation primarily originates from EU regulation and imposes a number of obligations on banks and other businesses such as pension companies, currency exchange offices, lawyers, auditors, insurance companies, etc. Denmark has furthermore tightened legislation to make Danish legislation one of the strictest in the EU.

These requirements reflect regulators' aim to put banks and other participants in the front line of detecting and reporting suspicious activity to the authorities. This is understandable as banks form such an essential part of society that they are required to take on greater responsibility on several fronts, and as they are in a position to detect money laundering and terrorist financing.

But let us take a closer look at the specific measures taken by banks to combat money laundering and terrorist financing.

AML policy and risk assessment

A bank's AML policy and risk assessment are the documents which set out the framework for its anti-money laundering efforts. In the risk assessment, a bank provides its assessment of the specific risk factors that determine the bank's risk of being misused for money laundering and terrorist financing based on the bank's business model. Risk factors include customer types, product types, services, geographical exposure, etc. Based on the risk assessment conclusions, the bank lays down the AML policy and the procedures to be initiated to mitigate any identified risks.

The AML policy generally lays down procedures to prevent and safeguard the bank against misuse for money laundering and terrorist financing purposes. The bank must, for instance, establish guidelines on its electronic as well as manual customer monitoring and procedures for disclosing that there are geographical areas within



which the bank will not operate or enter into business relationships etc. Within the AML policy framework, the bank must prepare business procedures or other procedures, detailing the bank's activities to combat money laundering and terrorist financing. Business procedures are a tool used by the employees, delineating the division of roles, responsibilities and how to perform tasks. Finally, controls must be established to ensure that the AML policy and business procedures are met. Together, these documents constitute the framework and procedures guiding a bank in the fight against money laundering and terrorist financing. It is a requirement under the Danish AML Act that the framework and the routines match a bank's specific business model, customer types etc and the related risks. Detailed and extensive work has been carried out by banks to prepare the documents above, which are individual to each bank.

Organisation of the fight against money laundering and terrorist financing

The fight against money laundering and terrorist financing takes up a large amount of resources at Danish banks, which is also evident from the way banks are or-

ganised. Estimates suggest that the six largest banks in Denmark combined employ about 4,300 AML and compliance staff tasked with monitoring and ensuring that banks are not misused for money laundering, terrorist financing or other financial crime. Staff numbers have been rising for a while and are expected to rise further going forward. Add to this staff in other job functions in the banks which are also involved in combatting money laundering and terrorist financing as part of their work. This includes customer advisers, for instance.

Efforts are moreover not just concentrated in one area but are integrated in several areas within the organisation to ensure that current practices in this area comply with legislation and the bank's internal rules. Banks' fight against money laundering and terrorist financing is modelled on the so-called three lines of defence:

Figur 4 Three Lines of Defence



1. The first line of defence includes the front office staff in the banks' branches who through their daily interaction with customers look for signs of money laundering or terrorist financing. Many banks also have a key AML unit, which considers the cases where for instance an adviser or the IT monitoring system has detected a risk of money laundering or terrorist financing.

2. The second line of defence are compliance and risk management units. The bank's compliance and risk management units are tasked with overseeing that the first line of defence meets the requirements laid down in legislation and the bank's business procedures and other procedures. This is done to ensure sufficient management of the bank's risks of being misused for money laundering or terrorist financing.

3. The third line of defence is typically an independent unit such as internal audit, which is tasked with verifying that the bank's lines of defence are adequate. In other words, they verify whether the first and second lines of defence work satisfactorily to counter money laundering and terrorist financing and comply with a bank's AML/CTF framework.

A bank's executive board has executive responsibility for combatting money laundering and terrorist financing. An executive board member will thus be responsible for ensuring that a bank implements and meets the requirements of the Danish AML Act by having effective policies, procedures and controls in place.

Moreover, under the Danish AML Act, banks must appoint an AML Responsible Officer to approve its AML policies, procedures and controls.⁵

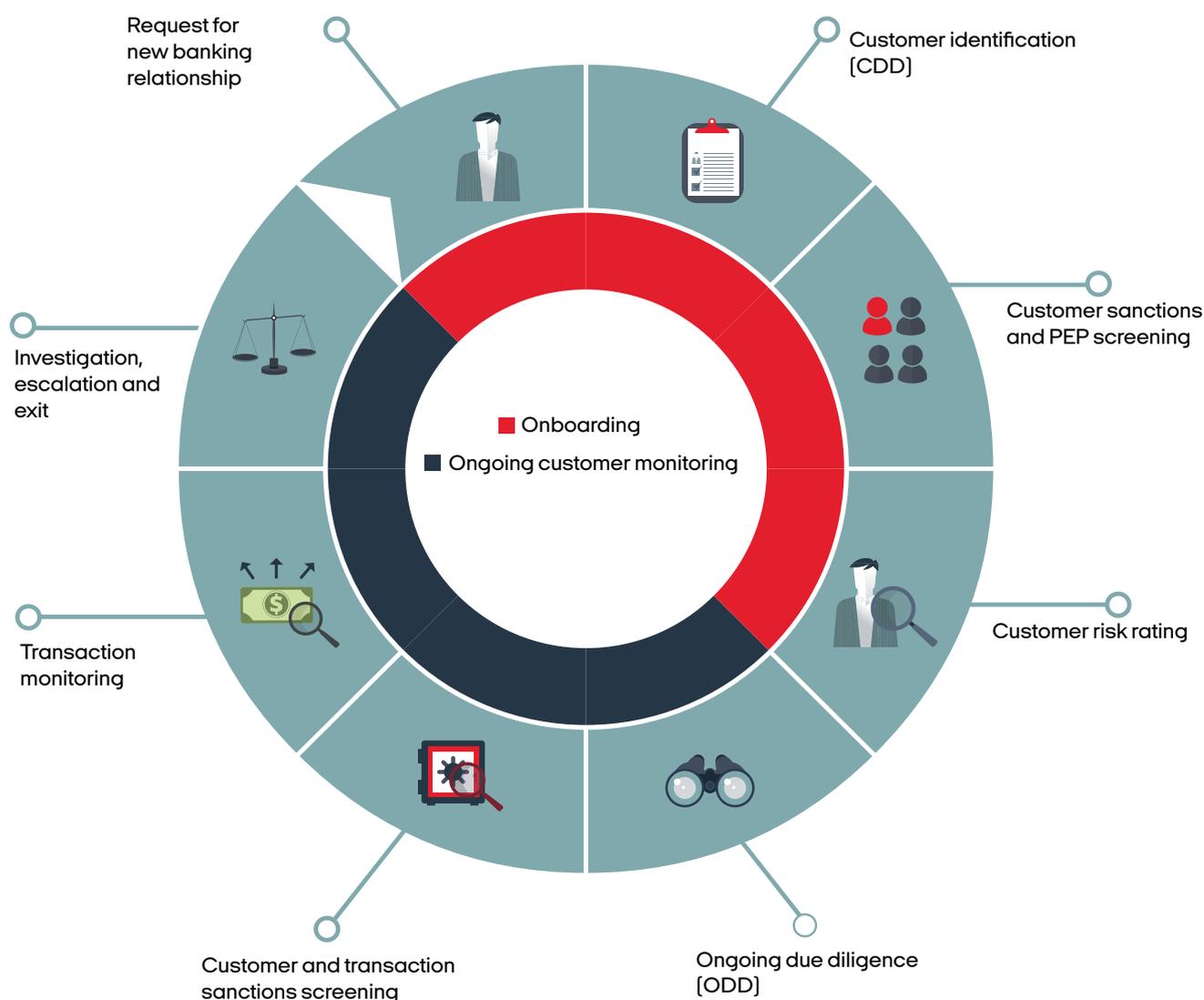
The AML Responsible Officer is also charged with approving correspondent relationships, ie relationships with other banks as well as customer relationships with politically exposed persons and their relatives and close associates.

In summary, beyond the daily contact with customers, banks allocate heavy resources to establish the best-suited organisation and the most effective business procedures in order to build the best defence against misuse for money laundering or terrorist financing purposes.

AML in the customer relationship

The fight against money laundering and terrorist financing is deeply integrated in the banks' customer relationships. The figure below outlines the different steps taken by banks when managing AML or CTF risks.

Figure 5 AML in the customer relationship



Source: Finance Denmark

⁵Branches of foreign banks are not required to appoint an AML Responsible Officer, cf section 7(2) of the Danish AML Act.

Know Your Customer (KYC)

Banks' interaction with customers is based on the key principle of "Know Your Customer [KYC]". Banks must have a wide knowledge of all their customers under the Danish AML Act, which will help counter misuse of the financial system, as they will be able to react in case of unusual customer behaviour.

In practice this means that banks must know the identity of their customers and the intended scope of the business relationship with the individual bank. Banks must know the name and civil registration number of a customer and obtain proof of evidence in this respect, for instance a copy of a customer's passport and national health insurance card. In case of new potential customers the bank screens customers and enquires about their identity, obtains documentation for the information provided and asks about the purpose and scope of the intended banking relationship. For instance, does a customer intend to raise a loan, open a current account or make international payment transfers? This information is essential for a bank to make a risk assessment of potential new customers and on this basis determine whether to accept such customers. Based on a bank's AML policy, controls and business procedures, the risk assessment helps determine which control measures the bank should take to counter the specific customer risk. Depending on a customer's risk score, banks will conduct ongoing customer due diligence at different frequencies, for instance annually for customers with an elevated risk level.

The amount of questions and documentation requirements for new customers may seem overwhelming, but must be seen in the light that in-depth customer knowledge is necessary for the bank to effectively monitor the bank's customer relationship and identify activity that may be linked to money laundering or terrorist financing. The bank's risk assessment of the individual customer is thus just as thorough as the bank's credit assessment of the customer. Although the risk associated with each individual customer relationship is low, it is necessary to collect information to ensure that the assessment is correct. The process can be compared with the security check performed at airports: everybody must be checked although each passenger poses a small risk.

It is a statutory requirement that the bank know and verify the name and civil registration number of a customer and the name and business registration number of a

business customer. This is indispensable. In addition, based on a risk assessment banks must ensure that they collect other relevant information to obtain sufficient customer knowledge. Relative to a bank's own risk assessment, it makes a discretionary assessment of what is relevant to ask about and obtain documentation for.

Once a customer relationship has been established, the bank will perform ongoing customer due diligence to assess, for instance, whether a customer's behaviour matches the information provided by the customer to the bank. If a customer's behaviour changes, for instance if a customer starts making transactions of a volume or scope that deviates from the information provided by the customer, a bank may expand its monitoring or ask additional questions. Banks will also ask about the source of funds, for instance if a customer receives an unusual payment. Banks must ensure that the customer information is updated regularly.

Monitoring of unusual circumstances

Banks may become aware of unusual circumstances that may give rise to suspicions in several ways.

Bank staff play an important role in the fight against money laundering and terrorist financing issues. They question and enquire about matters they do not understand when dealing with the customers. For instance, if a couple applying for a home loan informs their adviser that they have other income in addition to their salaries, this may suggest undeclared work. Banks strengthen the skills of their staff in this area through the training programmes which they are required to provide under the Danish AML Act. It is a requirement that management and staff working in areas that may be exposed to misuse complete these training programmes.

About 1.3 million instant and 850,000 intra-day clearing transactions are conducted daily in Denmark. The value of total transactions [sum, intra-day and instant clearing] is approximately DKK 4.1 bn on a daily basis, of which about DKK 1.2bn originates from instant clearing, where the transaction is executed within a few seconds without the involvement of a bank officer. This is why banks' monitoring of unusual transactions is highly dependent on automated digital monitoring. Over the past few years, banks have invested heavily in IT systems, facilitating banks' detection of unusual transactions. The IT systems enable capturing of atypical transactions.

Examples of information and documentation typically required of personal and business customers:

- Name
- Civil registration number or central business registration number
- Address
- Passport, driver's licence, health insurance card or birth certificate
- Purpose of the banking relationship
- The customer's expectations for the scope of the customer relationship with the bank
- Information and/or documentation of the source of customer funds
- The customer's income, for instance payslips, pension or public benefits
- The business customer's business purposes
- Information and/or documentation for business customer's ownership structure as well as beneficial owners. The business customer's provisions regulating the power to bind the entity or shareholders' agreements.





The Danish FIU refers reports to the relevant authorities; such as the Danish Security and Intelligence Service when there is a suspicion of terrorism, the national police in case of other crimes and Udbetaling Danmark when it comes to social benefits fraud [Note: most reports are transmitted to the Danish Security and Intelligence Service or the local police. The Danish Tax Agency receives reports on tax fraud. Udbetaling Danmark receives very limited reports on social benefits fraud].

For instance if the size of a transaction is unusual for the customer in question, the transaction will be singled out by the bank's staff for manual control. In most instances, it will be a false alarm, but in some instances the transaction cannot be cleared from suspicion.

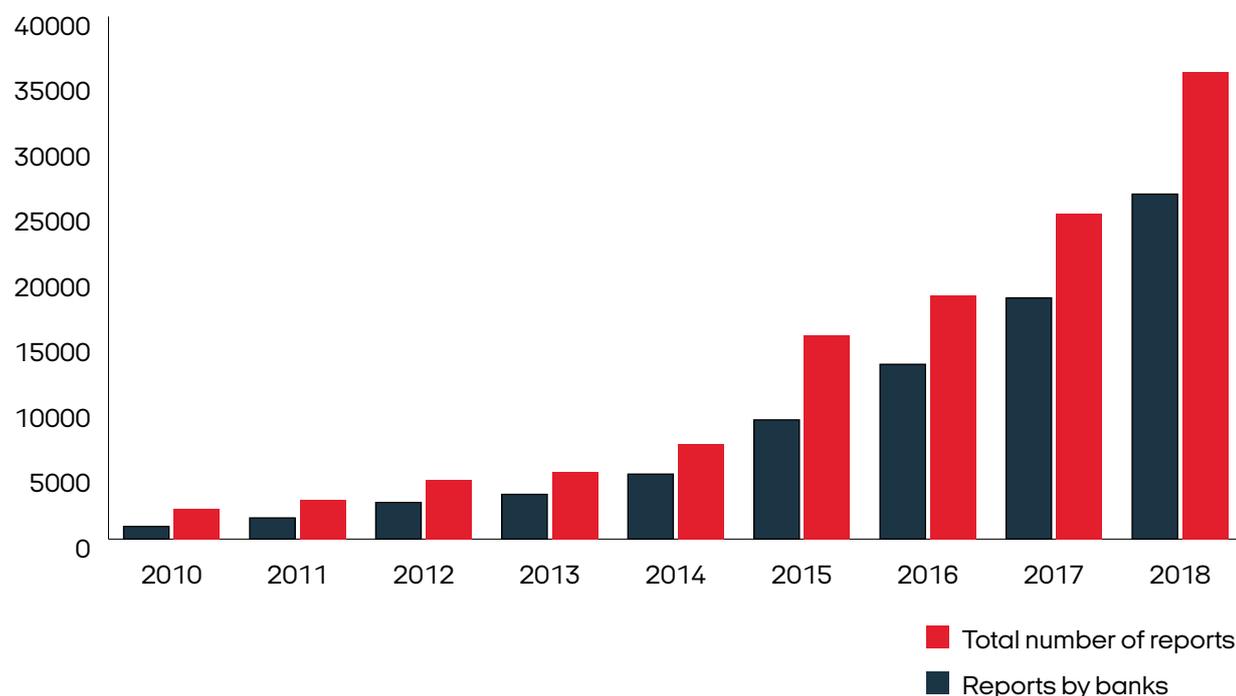
Reporting to authorities

If a transaction or behaviour appears unusual and cannot be cleared from suspicion of money laundering or terrorist financing, banks must report their suspicions to the authorities. Danish banks report suspicions to the Danish FIU, which screens the reports and refers reports involving other authorities to eg the Danish Security and Intelligence Service or the local police, the Danish Tax Agency or possibly Udbetaling Danmark.

Banks have reported a growing number of suspicious transactions over the past few years. Banks accounted for more than 26,000 of the total of 35,000 reports made in 2018. This represents a 43% rise on 2017 and as much as 189% relative to the 9,124 reports made in 2015.

Banks consequently account for the vast majority of reports made to the authorities; a trend which is expected to continue in 2019. In the first six months of 2019, Danish banks submitted more than 17,000 reports of a total of approximately 24,000, suggesting that the total number reported for the year will be around 35,000-40,000.

A question to be raised is whether all reports are useful to the authorities. The general feedback from the State Prosecutor for Serious Economic and International Crime is that the vast majority of the reports made by the sector are both qualified and screened and therefore provide a good basis for the authorities' further investigations. There is no indication that banks have made too many or unqualified reports. On the contrary, the authorities have indicated that they had grounds for doubting the justification of a report in only 5% of all reports made. An additional element of this discussion is that it is not up to banks but to the authorities to decide whether a report is useful, as banks are under an absolute obligation to report any suspicious behaviour.

Figure 6 Development in reports to the Danish FIU

Source: Chart based on data from the State Prosecutor for Serious Economic and International Crime.

The Danish FIU often uses the reports to compile a jigsaw of knowledge that may be of use in large cases. Although each single report does not lead to tangible results, it can often be highly useful as a piece in a jigsaw puzzle.

The Danish FIU's statement of reports filed and referred reports shows a 75% increase in the number of reports filed in 2018 from 2017, of which the majority of the reports have been sent to the Danish tax authorities. In 2018 information from 5,536 reports was passed on to the Danish tax authorities.⁶ The Danish Tax Agency states that the investigations and controls conducted on the basis of this information have resulted in significant net government proceeds.

Finance Denmark

Finance Denmark supports all initiatives aimed at combating financial crime. For this reason, Finance Denmark has played an active and constructive role and

attended various forums and negotiations when given the opportunity.

Externally, this means that Finance Denmark has discussed challenges and solutions with all political parties in the Danish Parliament, with ministry officials and with the Danish FSA. Finance Denmark has been a member of a council set up under KL – Local Government Denmark, tasked with determining the criteria for future contracts with banks. Finance Denmark participates in the Danish FSA's Anti-Money Laundering Forum+ and has generally strengthened its collaboration with the Danish tax authorities, the police, the Danish Security and Intelligence Service, etc. Finance Denmark has offered its services to the Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance [TAX3], which focuses on tax havens and anti-money laundering in the EU, cooperates with the European Banking Authority and is the Danish financial sector's contact vis-à-vis the FATF.

⁶ Source: <https://anklagemyndigheden.dk/sites/default/files/inline-files/Underretninger%20og%20videregivelser%202018.pdf>

Internally, Finance Denmark has launched the Anti-Money Laundering Task Force, which consists of external experts and internal experts from the Danish banks. Initiatives to strengthen the cooperation with the authorities have been launched, and quarterly meetings are now held between the banks, the State Prosecutor for Serious Economic and International Crime and the Danish FSA. This gives the Danish FSA's members an opportunity to have talks with the relevant authorities on the development in the area. We have also had good contact with the authorities in connection with the implementation of the Anti-Money Laundering Directives.

Moreover, Finance Denmark has appointed a permanent anti-money laundering working group charged with facilitating knowledge sharing with respect to legislation and best practice.

In addition to this are the numerous internal initiatives in the banks which each and independently of each other have stepped up their compliance efforts, launched campaigns for dialogue with the customers and filed considerably more reports with the Danish FIU.



CHALLENGES RELATING TO ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING

Even though the sector and the authorities do everything in their power to combat money laundering and terrorist financing, the fact remains that the threat of money laundering and terrorist financing cannot be eliminated completely. But why is it so difficult to combat the misuse of the financial system for money laundering or terrorist financing purposes?

It is hard to give a simple explanation. Professional criminals are skilled and intelligent. They keep up to date, and they develop new methods as they encounter new systems and technologies in the financial system. Criminal activities do not necessarily require physical contact but could be in the form of, for instance, buying or selling stolen information such as codes or data. If we look at organised crime, it is obvious that the criminals are quick to find new ways of misusing the financial system for financial crime. This invariably means that authorities and banks will often be lagging behind in the race to keep up with the newest methods used by criminals.

As emphasised in the National Risk Assessment by the State Prosecutor for Serious Economic and International Crime, the "process used to launder the proceeds of serious and organised crime involves a variety of methods, which are often quite complex and combine elements from both the legal and the illegal economy. The commingling of illegal and legal transactions takes place inter alia through banks, currency exchange offices, gambling providers, online funds transfer platforms,

international money remittance operators and a variety of business structures."

In other words, the combatting of money laundering and terrorist financing is a very complex area with many different participants. Historically, Danish society has been highly based on trust. Denmark is the best ranked country in the corruption perception index⁷, and bribery and corruption were never considered societal problems.

The concept of money laundering under the Danish AML Act covers everything from money laundering through complex international structures using shell and shadow companies to, for instance, tax evasion, social fraud and IT-related crime. The task therefore requires many resources and many different types of measures. There are many participants in the area, and many political measures and EU measures, as well as legislation that must generally be aligned with other rules and areas of law whose main purpose is not to combat financial crime.

The barrier that the financial sector must provide rests on the anti-money laundering legislation. The legislation provides the basic framework for organisation, business policies, practical business procedures etc. Customer due diligence is required, including verification of identity and obtaining an understanding of the services needed by the customer and why.

⁷Source: <https://www.transparency.org/cpi2018>

DILEMMAS

Despite the growing focus and the measures adopted in the area on an ongoing basis, the sector is still faced with some inherent dilemmas when acting as a gate-keeper to prevent and combat money laundering and terrorist financing.

IT solutions

Banks in Denmark have different IT systems. Danske Bank and Nordea operate with their own IT systems, and the other banks have outsourced many of the IT tasks to IT providers. 22 banks use BEC, nine banks use Bankdata, and a number of small and medium-sized banks in Denmark, Sweden, Norway, Finland and the Faroe Islands use SDC. Finally, there is JN Data, which is owned by the three IT providers together with Jyske Bank and Nykredit.

The IT systems have been developed and changed over time. They therefore include multiple solutions, reflecting an ongoing need for adjustments, changes and new measures.

The anti-money laundering legislation contains requirements that call for efficient IT solutions. For instance,

all customers must be identified and screened, and the information must be updated regularly. Considering the large amounts of customers, banks need IT solutions. The same applies to the requirements relating to monitoring of transactions, screening of customers against sanctions lists, screening of customers for PEPs and relatives of PEPs etc.

As combatting money laundering and terrorist financing is not a competition parameter, but a common corporate responsibility, the development of IT solutions is an obvious area for collaboration. A higher degree of integration of IT solutions going forward would make the sector's overall AML/CTF efforts more effective. This would benefit the IT systems, facilitating their adaptation to technological changes, and overall it would enhance the effectiveness of anti-money laundering measures, also in the long term.

Collaboration with authorities – conflicting interests

The overall purpose of the Danish AML Act is to prevent and combat money laundering and terrorist financing, and the Act therefore represents a broad and very



important societal commitment. However, in some respects the legitimate interests of the Act overlap, or are challenged by, the purposes and interests of other rules of law, including rules regarding data protection, consumer law, good business practice, duty of confidentiality etc. This gives rise to a number of dilemmas where the financial sector may be faced with conflicting interests, which are equally important, but cannot be equally allowed for in the specific situation.

The Danish AML Act is what is referred to in legal terms as "lex specialis", which means that it will, as a general rule, take precedence over any other conflicting law governing general matters. Consequently, a clear understanding of the scope of the rules of the Danish AML Act is essential to be able to determine that the rules and interests of the Danish AML Act take precedence over other rules and interests in a specific situation. It is therefore imperative that authorities dealing with such conflicting law ensure a uniform interpretation of the rules, providing a clear understanding in situations where rules of law overlap and where the interests of one area must yield to those of another.

Examples of practical dilemmas that may occur:

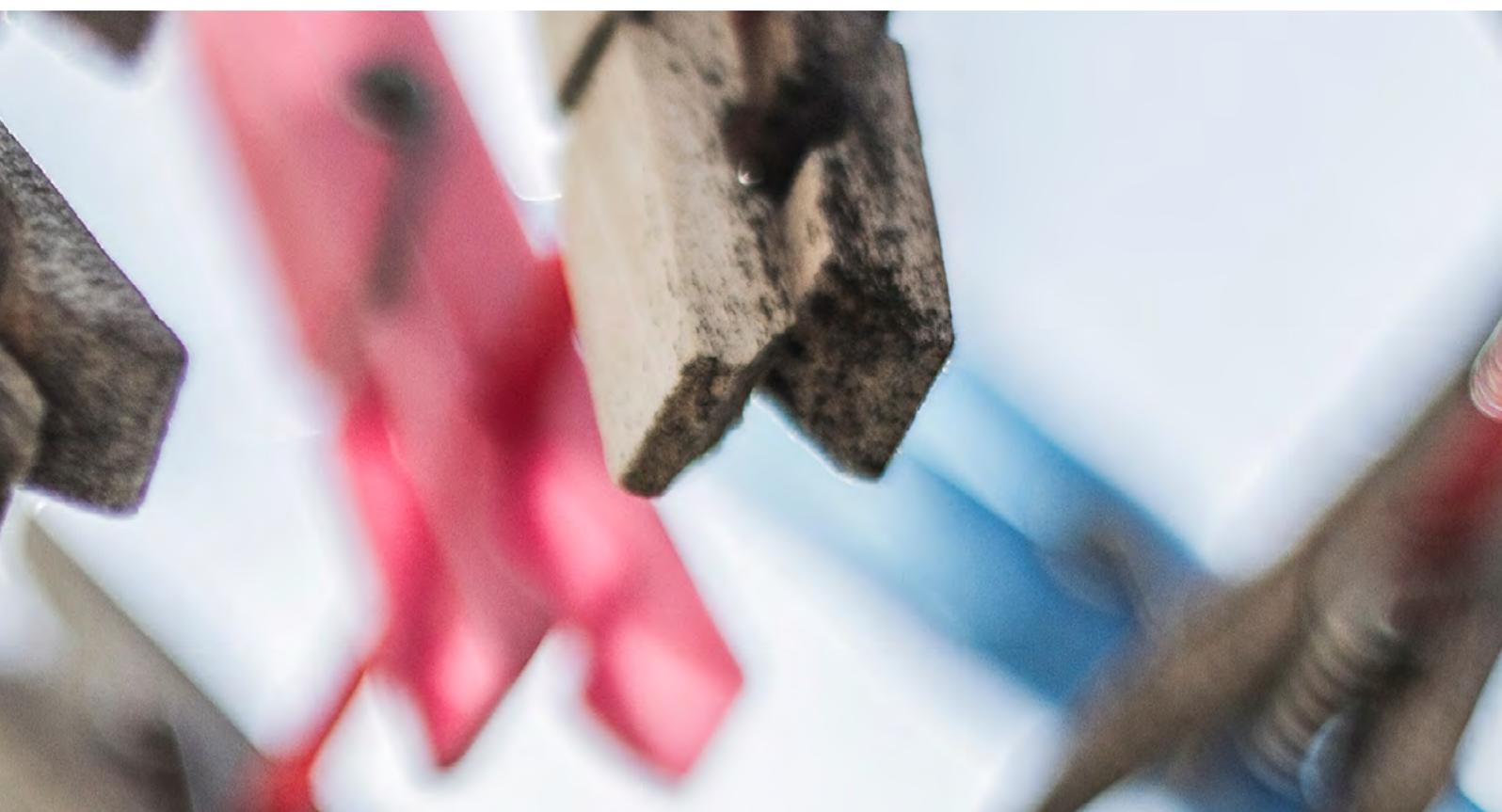
A private individual's right to open an account

A private individual has the right to open a basic payment account⁸. Services linked to basic payment accounts include making deposits, withdrawing cash, transferring funds, using payment cards and making direct debit payments. A basic payment account comes with an online banking solution, and the account can be used as NemKonto account. The services linked to a basic payment account are available from all EU/EEA member states.

This rule on the right to open a basic payment account may conflict with the rules of the Danish AML Act. The Danish AML Act prescribes that a bank must not enter into a customer relationship if customer due diligence cannot be carried out⁹. However, it has been decided that the due diligence requirements of the Danish AML Act take precedence. That illustrates the balancing act between a citizen's basic right on the one hand and the broad societal commitment linked to a bank's role as gatekeeper, protecting society against money laundering and terrorist financing, on the other.

⁸ Source: Section 11(1) of the Danish Payment Accounts Act.

⁹ Source: Section 14(5) of the Danish AML Act.



Customers' right to know the reason for rejection or termination

If a customer is rejected or a customer relationship is terminated, the customer is entitled to a motivated reason¹⁰, but at the same time, the Danish AML Act prescribes a duty of confidentiality when a bank suspects a customer and reports such suspicion to the Danish FIU¹¹.

The requirement of a motivated reason in case of termination is based on, for instance, the Danish Executive Order on Good Business Practice for Financial Undertakings. Furthermore, when the customer is a payment institution, a motivated reason is required under the Danish Payments Act.

A specific example is found in the Danish Payments Act¹², which stipulates a requirement relative to payment institutions when being bank customers. A payment institution is an undertaking that provides payment services. Examples of payment services are money transfers, mobile and online payments, as well as making deposits into or withdrawals from an account. According to the Danish Payments Act, banks must give payment institutions access to their payment accounts services on objective, non-discriminatory and proportionate terms. If a bank rejects a payment institution, it must notify the Danish Competition and Consumer Authority and provide duly motivated reasons for such rejection.

The requirement of the Danish Payments Act may pose challenges if, for example, a bank does not want to establish a customer relationship with a payment institution because of a concrete suspicion of money laundering. The bank will refuse the payment institution as a customer under the Danish AML Act and will report its suspicion to the Danish FIU. As a general rule, however, the bank will be required to notify the Danish Competition and Consumer Authority and provide duly motivated reasons for its rejection of the payment institution. The

bank cannot do that, as its suspicion in relation to the payment institution is subject to a duty of confidentiality.

Rules of the Danish AML Act on rejection or termination of a customer relationship

The rules of the Danish AML Act on rejecting or terminating a customer relationship are important to note in relation to the rules on good business practice, the right of private individuals to open a basic deposit account and payment account and the general right of customers to motivated reasons.

Under the Danish AML Act, a customer – personal or business – must be rejected, or the customer relationship terminated, if the customer due diligence requirements of the Act cannot be complied with.

However, this only becomes relevant after the bank has exhausted all possibilities of complying with the due diligence requirements of the Act¹³.

It follows that in cases where information obtained about a customer is inadequate or cannot be updated, banks must address the potential risk and consider whether to terminate the customer relationship¹⁴.

Under the Danish AML Act, there will consequently be situations in which a customer must be rejected, or the customer relationship must be terminated. It is up to the individual bank to determine when it has the right/duty to reject a customer once it has made every attempt to obtain the necessary information about the customer. Banks must here make a difficult assessment, which must also allow for the rights of the customer. Here, the practical problem is not conflicting rules, but doubt as to precisely when the rules are activated – banks are on their own when it comes to assessing exactly what constitutes appropriate measures, and the risk is that the authorities will later find that they made the wrong choice.

¹⁰ Kilde: section 43 of the Danish Financial Business Act, section 63(2) of the Danish Payments Act, sections 6(5) and 15 of the Danish Executive Order on Good Practice for Financial Undertakings.

¹¹ Kilde: section 38 of the Danish AML Act.

¹² Kilde: section 63(2) of the Danish Payments Act.

¹³ Kilde: section 14(5) of the Danish AML Act.

¹⁴ Kilde: section 15 of the Danish AML Act.

When suspicion stands alone

A particularly difficult dilemma occurs where a bank, in order to protect its reputation, does not want to enter into or maintain a customer relationship because of a suspicion, but has no legal grounds to terminate the relationship or reject the customer. An example: A customer is willing to provide the identity information requested, has documents proving the source of its assets, gives a legitimate purpose for using the bank and is otherwise cooperative. If, despite this, the bank suspects money laundering or terrorist financing in relation to such customer, will the bank then be entitled to reject the customer?

The dilemma can also occur otherwise; if a bank does not initially have a suspicion and a customer does not cause inconvenience to the bank, does not default on its obligations etc, but the bank later suspects the customer and reports its suspicion to the Danish FIU. In that situation, the bank's only ground for termination is this suspicion. If the suspicion is not of a nature requiring termination of the customer relationship, and the bank nevertheless decides to terminate the relationship to prevent potential misuse for money laundering activities, how should the bank explain the termination to the customer when the bank is under a duty of confidentiality concerning the suspicion?

On the one hand, banks must protect the interests of customers, but on the other, it must effectively prevent and combat money laundering and terrorist financing. A suspicion will often occur because the bank's monitoring systems generate an alert in respect of a customer. The bank will investigate the alert and determine whether the matter should be reported to the Danish FIU and whether other measures should be launched. With technological systems generating alerts based on scenarios indicating different risks, there is a risk of "false positives". These can often be dismissed when the reason for the alert has been investigated. However, there is a risk that a suspicion is reported and, in the extreme case, the customer relationship is terminated by the bank because of false positives, if the bank finds that there is a serious suspicion and risk in relation to the customer relationship, or that such suspicion and risk cannot be disproved.



This risk cannot be avoided when delivering on the societal commitment to combat money laundering and terrorist financing. Banks must be loyal to the role as gatekeeper and must prevent being used for money laundering and terrorist financing purposes. As described, this may lead to a customer being rejected because of an error of judgment. In order to have a thorough and reasonable due diligence procedure, such potential errors of judgment must be accepted.

A private individual's right to erasure of personal data

The data protection legislation provides a right to erasure of personal data¹⁵ and a principle of data minimisation to the effect that only relevant data limited to what is necessary¹⁶ are collected. This would seem to be challenged by the very unambiguous requirements of the Danish AML Act concerning data collection for the purpose of customer due diligence and storage of personal identity and verification data for up to five years after the customer relationship has ended¹⁷.

An example: A customer requests the erasure of personal data held by the bank concerning him or her, as the customer is moving abroad and wants to enter into a new banking relationship. The customer has been with the bank for 25 years, so the bank has a large amount of data on the customer, including copies of the customer's passport and all transaction statements. The bank is not allowed to erase the data as requested by the customer, as it is under an obligation to store the data for all 25 years plus another five years after the customer's relationship with the bank has ended.

This dilemma is thus not one between rules but between meeting the rules and meeting the customer's request. Politically, this is a question of prioritising between the conflicting interests of storing data for the purpose of combatting money laundering and terrorist financing on the one hand and the right of the persons concerned to privacy on the other.

The need for business accounts

Businesses need business accounts to operate and to pay salaries, settle VAT etc. Banks therefore play a crucial role in supporting the business sector and acting as facilitator.

Banks can only provide accounts to business customers, however, if they are able to obtain adequate knowledge of the customers. For instance, banks must know and obtain proof of a business customer's business registration (CVR) number, business purpose, organisation, ownership etc to be able to enter into a relationship with the customer.

Banks must therefore first understand and obtain proof of business customers' individual purposes, management and ownership structures (owners may be foreign citizens with foreign identification documents) etc. The bank must therefore weigh its commitment to society and the business sector against the need to obtain adequate knowledge of the customer.

Not all information in publicly available registers is verified, which makes it difficult for banks to verify identification data. This currently poses challenges in relation to shell companies

Duty of confidentiality/tipping-off and obligation to investigate unusual and complex matters

The Danish AML Act imposes an obligation on banks to investigate unusual and complex matters in detail. Also, the FATF recommends that all financial undertakings, including management and staff, be under an obligation not to disclose that a suspicious transaction or related information is reported to the Danish FIU ("tipping off"). Therefore, the Danish AML Act stipulates a duty of confidentiality, ensuring that an undertaking does not tip off a customer about having discovered the customer's suspicious and illegal actions or behaviour. The duty of confidentiality also covers any unusual matters where an adequate explanation is found, allowing the suspicion to be dismissed.

The rejection of a customer or termination of a customer relationship may also, in itself, give the customer an indication of suspicion. After reporting to the Danish FIU, a bank therefore sometimes has to maintain a customer relationship in order not to interfere with an ongoing investigation, even if the customer clearly continues its suspicious behaviour.

It appears from the Danish FSA's guidelines, however,

¹⁵ Source: article 17 of the General Data Protection Regulation.

¹⁶ Source: article 5(c) of the General Data Protection Regulation.

¹⁷ Source: section 30 of the Danish AML Act.

that if the bank finds that questioning the customer would tip off the customer about the investigation/suspicion, or it finds it inadvisable to contact the customer, it can refrain from doing so, and it must notify the Danish FIU immediately. It also appears from the guidelines that the customer's reaction may support a suspicion.

In other cases a customer may become suspicious anyhow, for instance if a bank asks questions about the matters that give it reason to investigate the customer. For instance, the bank may ask the customer why the customer has started making transactions with a country to which the customer has not previously transferred funds or from which it has not previously received funds, or why the customer has started depositing large cash amounts into its account. If the customer has criminal intentions, the customer may quickly find another bank and attempt to continue its activities there. As banks today are not able to exchange information on customers switching banks, it is not possible for the banks to prevent such traffic.

Exchange of information

The sector has strengthened its collaboration with the Danish FSA, the State Prosecutor for Serious Economic and International Crime, the Danish FIU, the Danish Security and Intelligence Service and the Danish Tax

Agency. Finance Denmark has also set up a forum where Danish authorities and banks regularly meet to discuss the best ways to combat money laundering and terrorist financing. Here, the Danish FIU gives feedback on banks' reports.

However, the exchange of information is still far from efficient. If a bank rejects a potential customer because of a strong suspicion of eg money laundering, the bank will report the suspicion to the Danish FIU. But under current law, it is not possible to warn other banks against this customer.

In other words, if a bank rejects a customer on the grounds of money laundering, and the customer then contacts the bank "next door", the bank will not be able to warn the new bank that the customer is likely involved in money laundering or terrorist financing. This renders the system less effective, see Figures 7, 8 and 9 below.

On the other hand, it is a difficult balancing act, as customers have a basic and justified right to confidential treatment of their data. As will be illustrated later in this report, there is consequently a need to find a solution that allows for both the interests of the individual customer and the commitment to combatting money laundering and terrorist financing effectively.

Figur 7 Banks cannot warn other banks

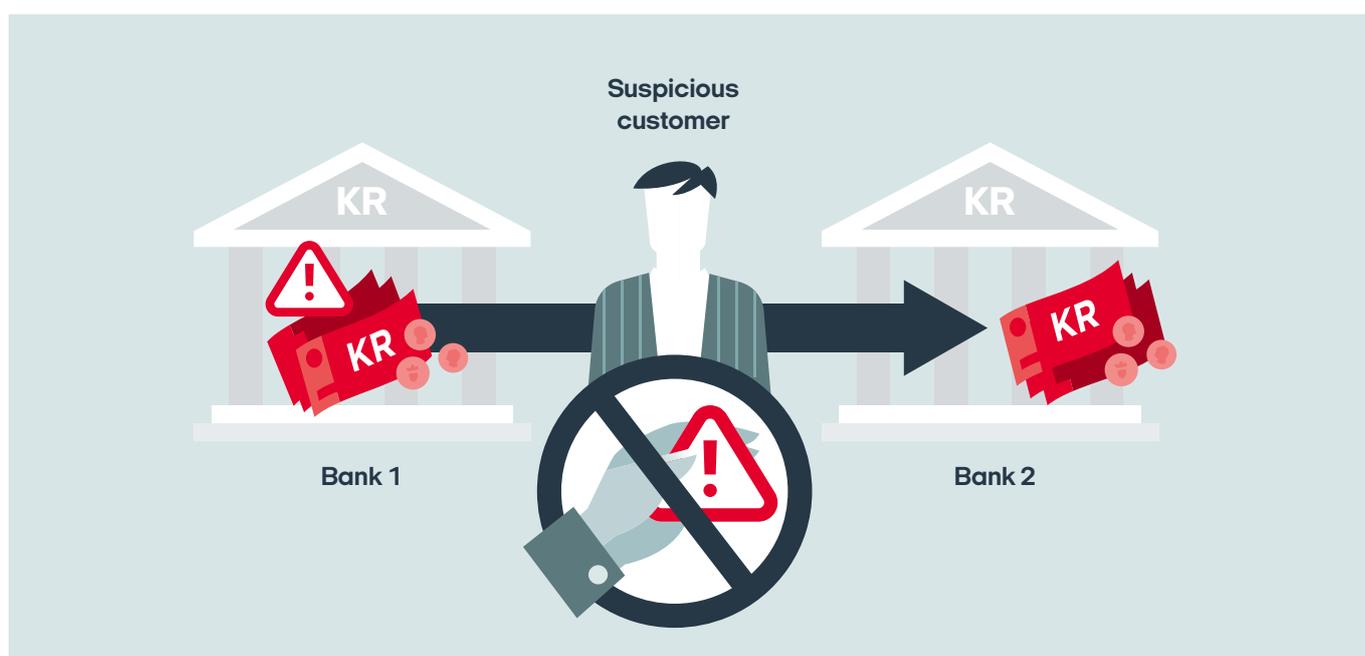


Figure 8 Barriers posed by the duty of confidentiality

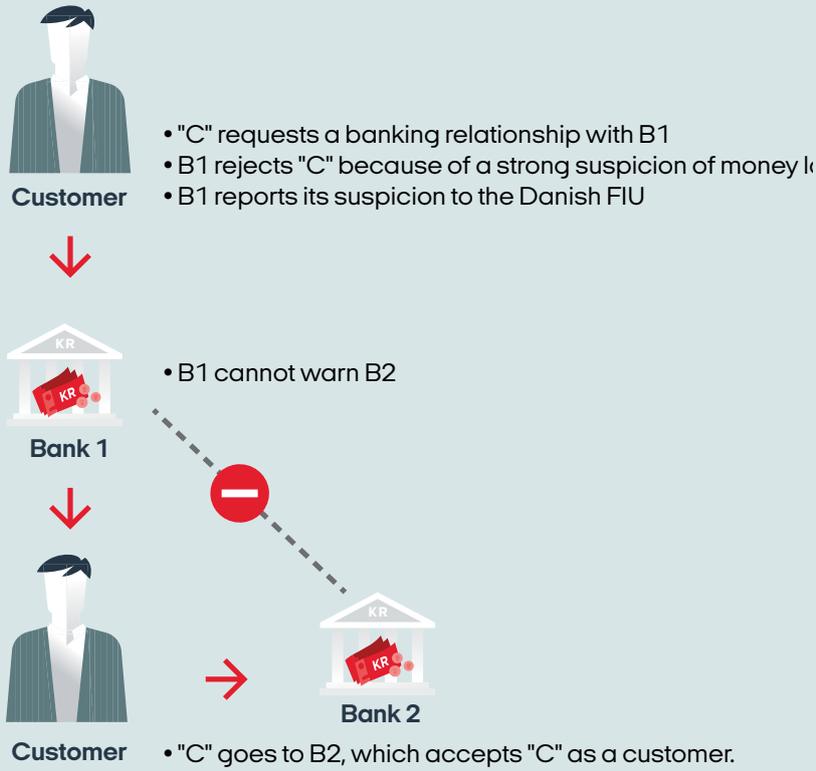
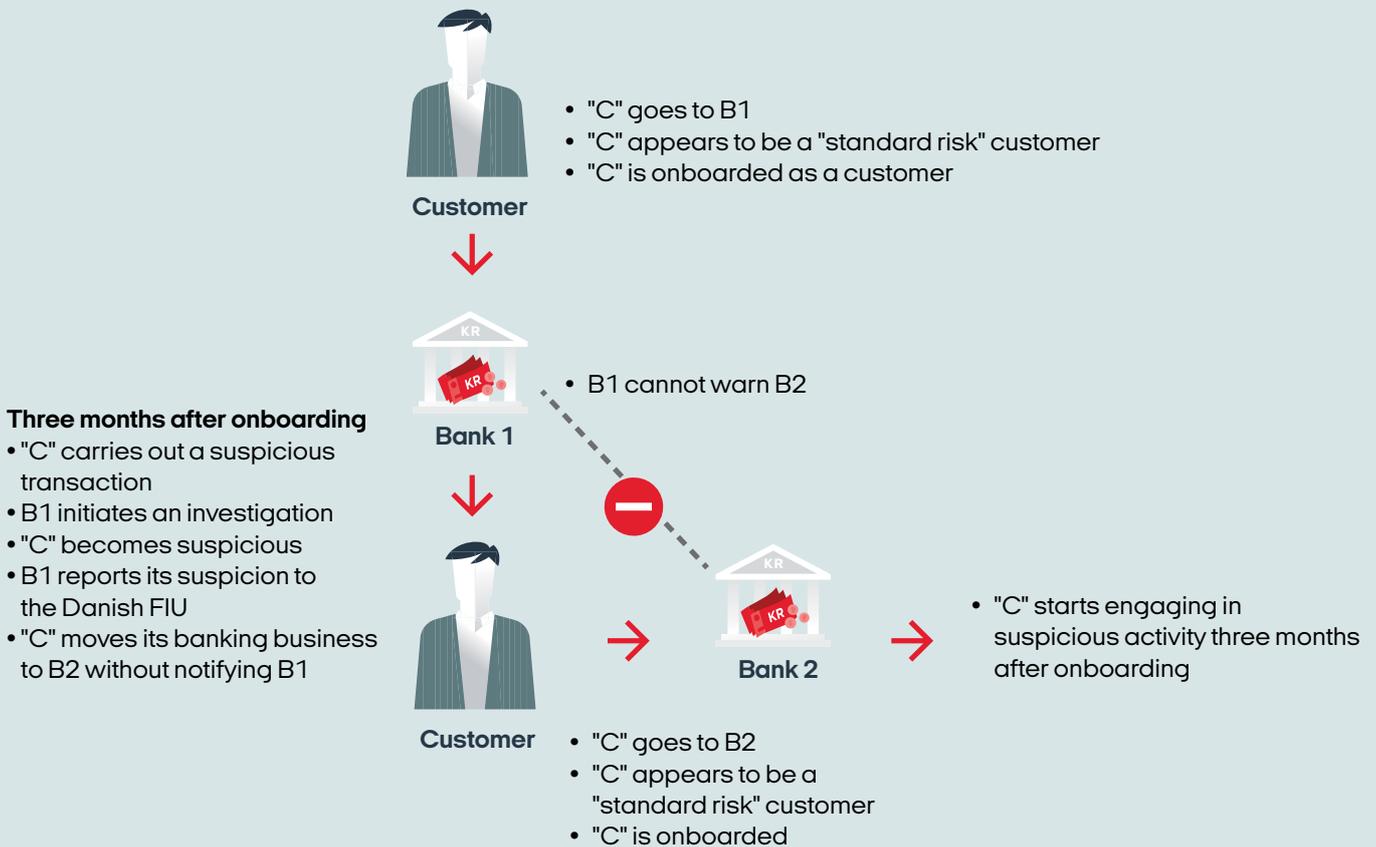
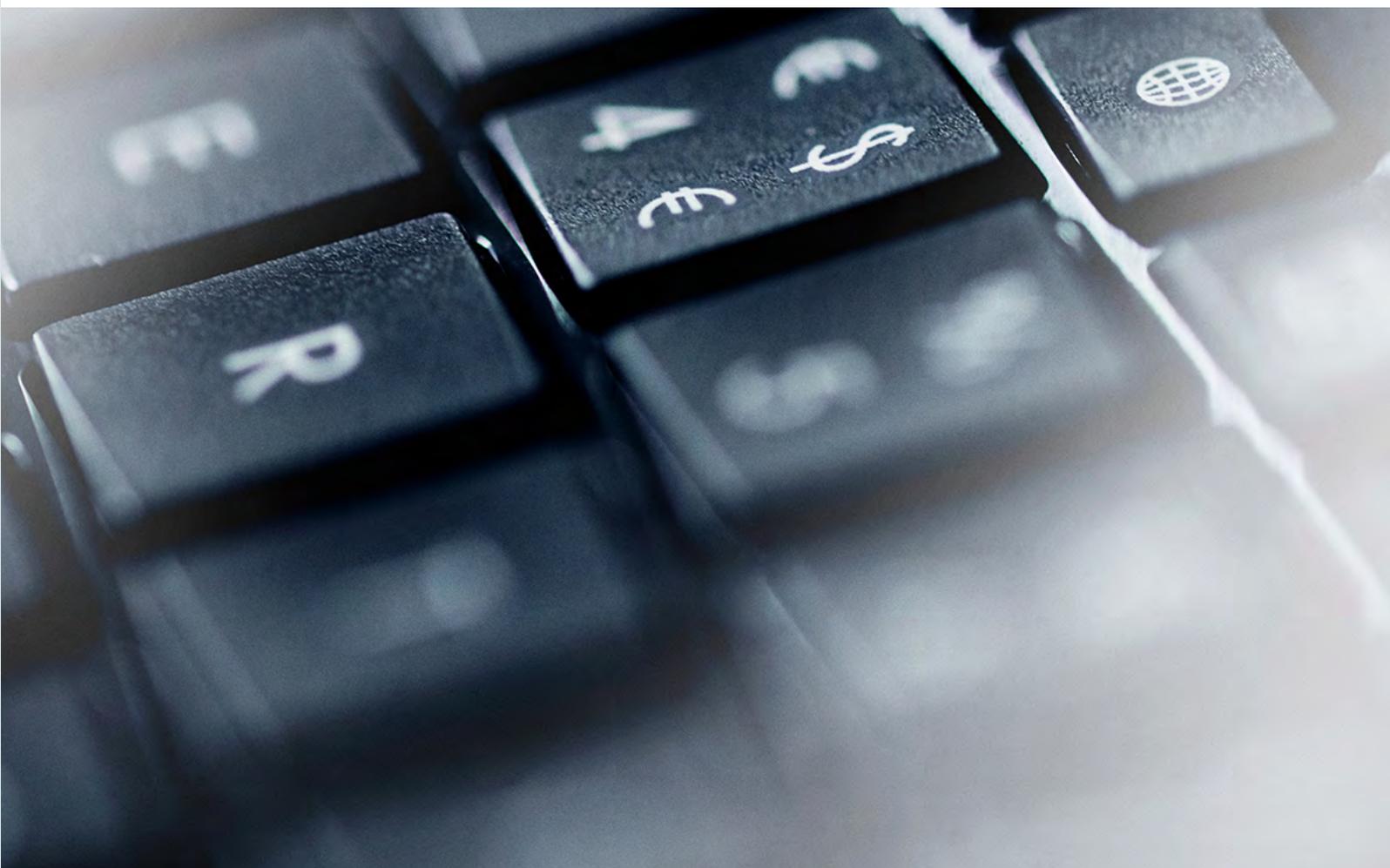


Figure 9 Barriers posed by the duty of confidentiality, expanded





Other situations that may give rise to suspicion

The fight against money laundering and terrorist financing through the financial system as described above creates situations with difficult dilemmas. Responding to suspicions may be of benefit to society, but it may also be to the detriment of the customer if the suspicion turns out to be unfounded. Banks are often caught between several interests, and this gives rise to daily dilemmas in the efforts to combat money laundering and terrorist financing.

Additional situations that may give rise to suspicion:

- A customer deposits a large amount into his account, explaining that he won it at a casino.
- A customer wants to open an account and provides the necessary information to the bank, but the customer will not or cannot provide proof of origin of his funds. The customer considers this to be private information.
- A customer opens a basic deposit account for wage transfers, but unusual transactions are made in the account; the customer then leaves the country, and the bank is unable to reach him.
- Via borger.dk a person has selected a third party's NemKonto account as his NemKonto account; there is no requirement that you must be the holder of your NemKonto account. The holder of the account and the receiver of, for instance, public benefits in the account are now two different persons. This means that the bank may not know the person operating the account, as the bank has established a customer relationship with the holder of the NemKonto account.
- A large amount of transactions are made between business undertakings where the connection does not seem logical.
- The revenue in a company's account is exceptionally high considering the company's turnover of goods or services.
- A company has been established but has no significant activity and few transactions in its account.



RECOMMENDATIONS OF THE ANTI-MONEY LAUNDERING TASK FORCE

The work of the Task Force over the past 11 months was divided into five main tracks:

1. Joint IT solutions
2. Stronger partnerships with authorities
3. Training
4. Self-regulation in the form of principles of conduct
5. Increased transparency

Based on the current situation, a needs analysis and an assessment of possible initiatives, the Task Force has drawn up a number of recommendations for the five main tracks. These are supplemented with a section on

additional sector initiatives. Together, the recommendations constitute a large catalogue of initiatives.

Since combatting money laundering and terrorist financing is a societal responsibility, the report also includes proposals for political initiatives to optimise the efforts. The aim is for the sector, in partnership with authorities and politicians, to become a front runner in the fight against money laundering and terrorist financing in the same way as Denmark stands out in terms of, for instance, anti-corruption.

MAIN TRACK 1:

JOINT IT SOLUTIONS

The expansion of joint IT solutions is a key theme. Like the public sector, banks have been quick and efficient to adopt digital solutions. Besides, joint industry-wide solutions have been part of the DNA of banks in other areas.

In recent years, preventing and combatting money laundering and terrorist financing have become an increasingly important part of banks' activities. This area, too, widely uses IT solutions, combined with a very significant use of human resources. IT solutions in this area have tended to be silo-based, with the three IT providers BEC, Bankdata and SDC as well as Danske Bank and Nordea each developing their own solutions to the money laundering and terrorist financing challenges. This applies to "Know Your Customer" (KYC) or "Customer Due Diligence" (CDD), transaction monitoring, reporting to the Danish FIU, etc.

However, the time has come to analyse the opportunities of expanding the joint anti-money laundering IT solutions. This area should not be the object of competition between banks, but should be an area of collaboration for the purpose of fulfilling the social contract for the prevention and combatting of financial crime in a broad sense, including money laundering and terrorist financing. The same goes for compliance with current legislation.

Only by collaborating to ensure effective IT solutions can we win the joint fight of banks and society against money laundering

From an overall perspective, the establishment of far more joint bank IT solutions will offer a number of advantages in terms of preventing and combatting money laundering. It would be cost-efficient, it would make AML/CTF collaboration easier and more efficient, and being technologically advanced would improve the chances of combatting financial crime and matching the criminals.

At the same time, joint IT solutions should take into consideration that "one size fits all" does not necessarily apply at all levels; banks have different sizes, different business models, different customers etc. The trick is therefore to translate banks' diversity into formulas and standards for the purpose of AML activities while at the same time allowing to some extent for their differences. To this end, it must be possible to calibrate the joint IT systems according to the different needs of the different banks. However, the future AML collaboration requires a standardised AML approach, serving as a common platform for the fight against money laundering where all banks have minimum AML standards, and standardised solutions are applied wherever possible. This would also protect against financial criminals looking to target the "weakest link".

Standardisation will also significantly simplify collaboration with the authorities, which will be imperative in future.

It is important that banks already now prepare for the introduction of new technological solutions in the area. The use of learning algorithms, machine learning and artificial intelligence (AI) is expected to become an essential part of AML activities and compliance within the foreseeable future, and as in so many other areas, readiness to embrace the solutions when they come is important. This means that banks should make sure already now that sufficient, relevant and valid data including good processes and the necessary documentation are in place to allow the launch of learning processes enabled by the new technologies.

The Task Force's recommendations for more joint IT solutions can be divided into three layers:

1. A minimum solution involving five specific IT projects to enhance efficiency.
2. An expansion of industry-wide AML systems.
3. A vision of industry-wide IT collaboration by 2025.

The Danish financial sector has a long history of working together to solve non-competitive tasks. Partnerships exist across the sector as a whole, between groups of banks with shared needs, and as joint public-sector/private-sector partnerships. See below for examples of such partnerships. The list is not exhaustive.

Joint industry-wide solutions

- The Danish systems for clearing and settling retail payments: sum clearing, intra-day clearing [from 2013] and instant clearing [from 2014]
- Dankort [payment card], established in 1983
- Direct debit [“Betalingsservice”], operational from 1974 under the name of PBS [“Pengeinstitutternes BetalingsService”]
- VP Securities, owned by banks, mortgage lenders, stockbrokers, Danmarks Nationalbank and issuers, established in 1980
- e-engagement – automated bank switches since 2015
- NFCERT – Nordic Financial CERT [Computer Emergency Rescue Team] for sharing knowledge about cyber threats. NFCERT originally started as a Norwegian financial CERT, but it now includes all Nordic countries, and in Denmark, Iceland and Norway, most banks are members.

Joint solutions for groups of banks

- The three bank-owned IT providers SDC, BEC and Bankdata, established in 1963, 1965 and 1966, respectively
- BOKIS [“Betaling- Og KortIndkøbsSamarbejdet”]. The company’s purpose is to carry on business arranging licences to issue payment cards and operate payment solutions and acquiring and offering related services to the members of

local and national bank associations [LOPI and LDB].

Joint public-sector/private-sector solutions

- NemKonto, operational from 2005. NemKonto is the account which all public authorities and many private operators use when making payments to Danish citizens.
- Digital land registration – digitisation of the previously paper-based registration process, operational from 2009.
- NemID, operational from 2010
- NemID code app; almost 2.6 million users have downloaded the app since its launch in 2018
- MitID, to replace NemID in 2021/2022.

Joint solutions in the pipeline

- Nordic KYC Utility, an independent business owned by the six largest Nordic banks for the purpose of developing uniform on-boarding [KYC] processes for corporate customers, expected to be operational from mid-2020
- P27, pan-Nordic clearing in DKK, SEK, NOK and EUR [Iceland is not part of the project]. The owners of P27 are the six largest Nordic banks. Expected to be operational from mid-2021.

Five industry-wide AML IT projects to be launched now – as a minimum solution

e-nettet, the financial sector's digitisation company, was asked by the board of directors of Finance Denmark in the summer of 2019 to explore the scope for industry-wide AML/CTF solutions and submit proposals for specific initiatives.

Against that background, the Task Force proposes that five concrete projects, centred around the KYC principle, be implemented within the framework of e-nettet as soon as possible.

1. KYC (Know Your Customer) – common AML/CTF standard

This is one of the cornerstones when it comes to strengthening cross-sector collaboration, as it provides for standard definitions of eg purpose, scope and customer risk assessment, thereby raising quality.

2. Passport validation

A number of passport readers are available in the market today. However, the existing solutions only serve to verify whether a passport is genuine or fake. e-nettet will provide a solution that also checks whether there is a valid match between a person's civil registration (CPR) number and passport number. An industry-wide solution will enable banks to check for matches between CPR and passport number in the Central Passport Register.

3. PEP/RCA register

There are quite a few service providers that offer to screen for PEPs (politically exposed persons) and against sanctions lists. However, their screening of relatives and close associates (RCAs) of PEPs is not efficient and consequently exceptionally resource-intensive. The Task Force is of the opinion that this problem, which is common to all banks, should be solved jointly, as a joint solution would be more efficient than each bank performing its own screening. The Task

Force also believes that such screening should be the responsibility of the authorities, as it is very difficult for banks to obtain the relevant information, which is highly inaccessible and unreliable, and as a register of PEPs and their RCAs would fall naturally within the remit of public authorities.

4. Joint data register

The Task Force proposes a new joint register compiling data from the above three projects. This would place the sector in a stronger position, especially in terms of identifying persons who attempt to commit financial crime in one bank and then attempt to do the same, only in another bank.

5. Account ownership portal

The EU Fifth Anti-Money Laundering Directive requires an IT solution that will enable investigation authorities such as the Danish Security and Intelligence Service and the State Prosecutor for Serious Economic and International Crime to quickly retrieve information on account or safe-deposit box holders. Such information is key to investigations as it allows, for example, the identification of persons involved in a series of suspicious transactions. The authorities can access this information already now. However, that requires a court order, and the information is not gathered in one place. The sector considers it an important task to assist the authorities in procuring the necessary information. An account ownership register holds great potential in terms of allowing the authorities to get access to relevant information in time for them to seize the funds of criminals before they are moved. The sector, in this context Finance Denmark, has therefore decided to undertake the development of the solution in partnership with the authorities and to pay the development costs.

In response to the increasingly globalised and digitised nature of crime, more information is collected today than previously for the purpose of combatting cybercrime, other types of cross-border crime, including money laundering and terrorist financing, and other crime that will be combatted more simply and efficiently through data sharing.

In response to the increasingly globalised and digitised nature of crime, more information is collected today than previously for the purpose of combatting cybercrime, other types of cross-border crime, including money laundering and terrorist financing, and other crime that will be combatted more simply and efficiently through data sharing.

Projects to expand industry-wide AML systems

Expanding industry-wide IT solutions and their implementation will take more time. They will require substantial resources, massive investments, basic agreement on scope etc. Nevertheless, there is hardly any doubt that joint IT solutions would benefit the sector and its reputation, and also, this very type of investment is expected to pay for itself.

It is the ambition of both politicians and the industry that Denmark should position itself as forward-looking and proactive in the AML area. Substantial efficiency improvements and financial savings can be achieved by joining forces; joint sector investments will result in a more efficient defence against money laundering and terrorist financing than if investing separately and at different paces.

Against that background, the Task Force recommends wider collaboration on joint IT solutions to combat money laundering – and potentially wider efforts to combat

financial crime. Since this will be a process potentially requiring massive investments, keen skills and considerable work, it is recommended that the sector now lay down specific visions for the use of joint IT solutions.

Vision of industry-wide AML collaboration 2025

The process has been motivated by a common vision of industry-wide AML, based on the recognition that AML should not be a parameter of competition, but a common vision involving several joint IT solutions and increased sector collaboration. This will also make it easier to keep step with the creativity of criminals in terms of new methods of money laundering and terrorist financing. As regards commitment to an industry-wide AML system, all members of Finance Denmark have declared themselves willing to contribute knowledge to the extent required by the project. They will contribute data according to the specifications agreed by the sector and as necessary to build value-adding solutions for the sector in general. In this context, Finance Denmark has asked e-nettet to prepare a proposal for a long-term vision of industry-wide AML collaboration 2025. The overall vision is to combat and prevent money laundering and terrorist financing using digital and data-driven solutions based on a partnership between the financial sector and the public sector. The underlying objectives of the vision is to increase confidence in the financial sector, to facilitate the daily interaction between banks and their customers, to strengthen collaboration with the public sector, to reduce the costs incurred by banks and thereby to make Denmark a pioneer in industry-wide collaboration.



Figur 10 AML / CFT Vision 2025

VISION FOR INDUSTRY-WIDE AML/CTF PROGRAMME

The long-term vision will set the course for industry-wide solutions over the coming years.

THROUGH THIS VISION, WE AIM TO:

01

Restore the social contract and improve confidence in the financial sector's commitment to fighting money laundering and terrorist financing.

- Ensure high standards of ethics and responsibility in the joint efforts to combat money laundering and terrorist financing.
- Industry-wide efforts will send a strong signal that the sector is ambitious and determined to change its approach in the fight against money laundering and terrorist financing. This will improve the sector's image and strengthen the social contract.



02

Make the daily interaction with banks of citizens and businesses easier, while at the same time it becomes harder to launder money and finance terrorism due to the sector's high common standards.

- Digitisation and standardisation will enable the sector to share knowledge in real time, making it easier for customers to share data and information with their bank.
- Moreover, the centralised services will raise the sector's security and compliance bar, making it harder for criminals to find weak links to exploit.

AML VISION 2025



To combat and prevent money laundering and terrorist financing using digital and data-driven solutions based on a partnership between the financial sector and the public sector.

03

Be a pioneer in industry-wide collaboration and use of technology, benefiting the financial sector and the Danish society alike.

- Collaboration facilitates cheaper and faster introduction of new technologies throughout the sector.
- The use of new and smarter technologies such as biometrics, robots, artificial intelligence and advanced workflow tools through a central service will facilitate cheaper and faster processing of large amounts of data and make efforts to combat money laundering and terrorist financing more effective.

04

Enhance collaboration with the public sector, making the reporting and investigation of suspicious behaviour more efficient and supporting the restoration of the social contract.

- Meeting the social obligation calls for societal tools. Stronger partnerships between authorities and the financial sector will promote the development of the necessary solutions.
- Legislative changes and collaboration on requirements for IT solutions will underpin standardisation and the real-time exchange of data between authorities and the financial sector.

05

Reduce the costs of Danish banks through digitisation, standardisation and economies of scale.

- Enhanced cross-sector collaboration will pave the way for digitisation and automation of the entire AML/CTF ecosystem through centralised services. This will eliminate manual processes, reducing costs substantially compared with today.

To realise the vision, a specific proposal is made for a shared industry utility to be set up to in the form of a "jointly owned service utility to streamline the collection, verification, storing and sharing of data and documents, supporting the sector's AML/CTF procedures and processes. In the longer term, more processes and procedures could be centralised in the utility."



Figure 11 A shared industry utility

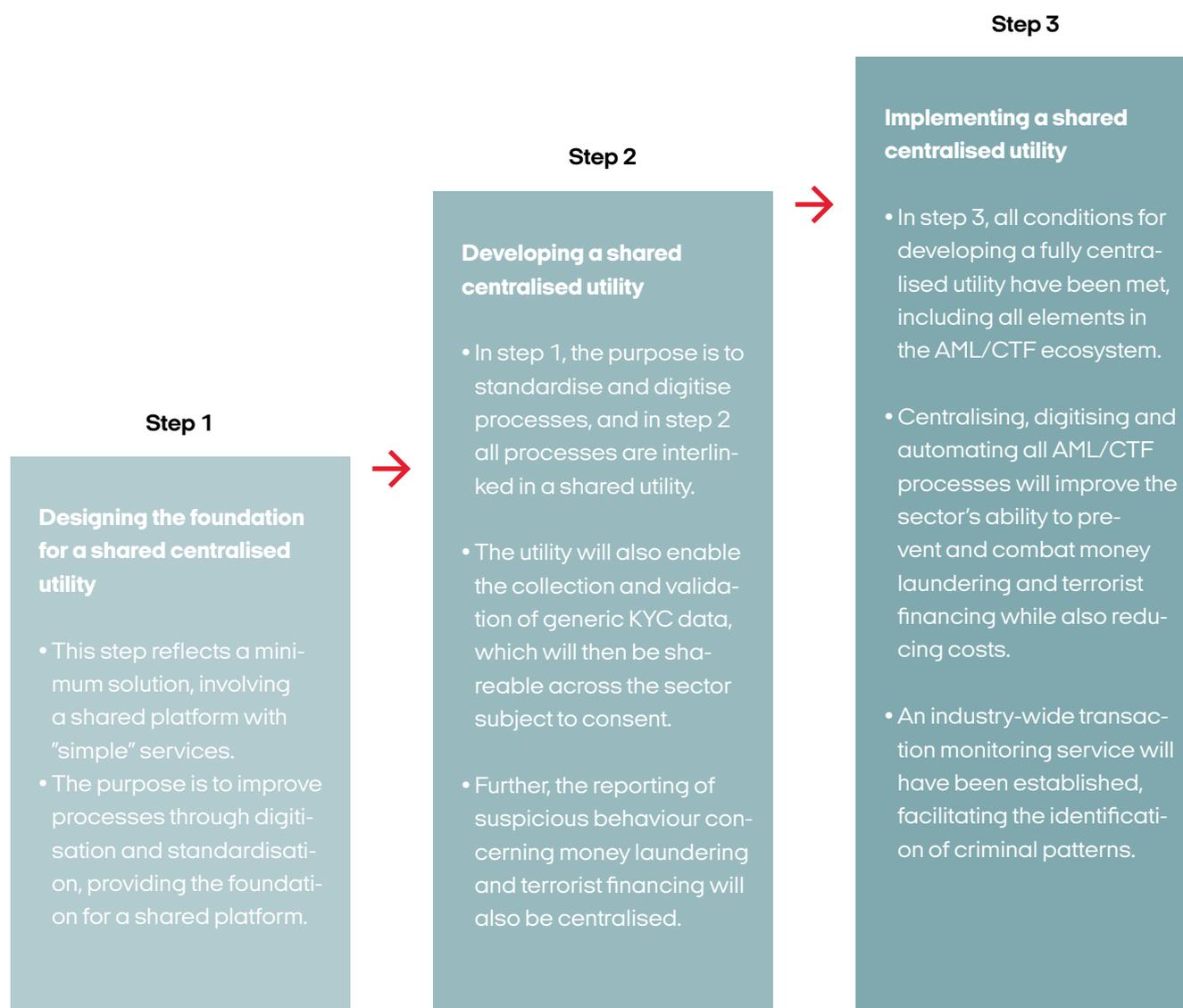
A SHARED INDUSTRY UTILITY IS THE SOLUTION TO ACHIEVE THE VISION

It is a solution involving many steps, and now is the time to invest in future solutions

WHAT MAKES A UTILITY THE ANSWER TO THE VISION?

- The financial sector must rethink its approach to fighting money laundering and terrorist financing. Driven by a growing pressure for change from both internal and external forces, combined with a greater willingness to accept responsibility, the time has come to change the status quo.
- The need for change, combined with a complex inter-linked AML/CTF ecosystem, makes a shared industry utility the only long-term solution that can meet the requirements, mitigate the problems and offer tools that support all ecosystem processes.
- Moreover, a shared centralised utility will offer digital and data-driven solutions increasing standardisation and automation in the AML/CTF area across the sector.
- It is important to note that building a shared industry utility will not be according to a completely linear, pre-defined road map. To achieve the vision, all sector participants must commit to the course and engage in a solution that will benefit all.

THE JOURNEY TO ACHIEVE THE VISION



Involvement of stakeholders with a particular focus on the public sector

Legislative changes

Digitisation and automation

Building the structure and foundation of a utility

Communication



There are already several examples of shared industry utilities. The six largest Nordic banks have joined forces in the Nordic KYC Utility to set up an independent legal entity charged with collecting, validating and sharing generic KYC data concerning the largest corporations in the Nordic countries. The utility will make it simpler for customers to deliver the data to financial institutions that are needed to identify any unusual or suspicious transactions and reduce the costs incurred by the sector in the efforts to collect and validate data from large corporate customers.

The number of reports filed over the past few years has just kept growing, and the trend is not likely to end any time soon. This underlines the importance of shared efforts to find efficient and cost-effective solutions. The work to set up efficient, shared IT support and centralised processes therefore requires increased collaboration with the public sector, in terms of both the establishment and use of new solutions and the need for legislative adjustments. Going forward, the development of IT solutions will therefore be closely linked to the Task Force's second track, stronger partnerships with authorities.

The proposed shared industry utility could be a jointly owned service utility charged with, for example, stream-

lining the collection, verification, storing and sharing of data where this is compatible with the requirements for banks' individual data processing, thereby supporting the sector's AML/CTF processes. The process of developing the utility can be divided into steps: The first step forms the basis of minimum solutions and provides for initial preparatory works, thus creating the foundation for the vision. The next step is where development takes place and processes are linked and where ideas to expand minimum solutions and develop new IT solutions are launched. This includes the collection and validation of generic due diligence data. The last step builds on the implementation of a fully centralised utility, operating and handling all joint digitised and automated solutions identified as possible in the preliminary analysis, for instance industry-wide transaction monitoring.

The Task Force's recommendation of long-term, comprehensive, industry-wide AML/CTF collaboration is very ambitious, and many technical and regulatory challenges will have to be overcome in the process. For instance, legislative changes will be required for banks to be able to share customer data. The Task Force therefore recommends the immediate launch of a pre-project to identify precisely what is required to realise the vision.

The General Data Protection Regulation (GDPR)

- Disclosure of personal data regarding a specific customer constitutes processing of personal data for the purpose of the General Data Protection Regulation (GDPR) and is consequently subject to restrictions. Personal data processing usually requires consent, and the relevant person will have a number of rights, such as right of access etc.
- However, the GDPR includes a number of exemptions allowing processing without consent where, for example, tasks are carried out in the public interest. Moreover, measures can be introduced at national level allowing derogation from the rights conferred by the GDPR. This is the case, for instance, in connection with authority measures to combat crime.

MAIN TRACK 2:

STRONGER PARTNERSHIPS WITH AUTHORITIES

The Task Force is of the opinion that efficient prevention of money laundering and terrorist financing requires substantial joint efforts by the sector and the authorities to create as intelligent and fine-meshed IT systems as possible, providing as broad a common framework as possible.

The partnership between the financial sector and the authorities is thus fundamental and key to the success of combatting money laundering, terrorist financing and other financial crime.

In the interest of corporate responsibility and the social contract, it should be a fundamental principle that the same AML/CTF tools are made available to banks as are available to authorities. In other words: A social contract calls for societal tools. This forms the basis of many of the proposals listed below.

The past few years have seen significant expansion and improvement of the collaboration on the general conditions for combatting money laundering and terrorist financing. This applies to inter-authority collabora-

tion as well as collaboration between authorities and private participants. However, priority should be given to reviewing regularly how the partnerships can be strengthened even further.

Why expanded collaboration between authorities and banks is important – and difficult

Many of the authorities involved in anti-money laundering and counter-terrorist financing initiatives have their own individual characteristics and IT systems.

Some relevant data are held by the Danish FIU, some by the Danish Security and Intelligence Service, some by the Danish FSA, some by the Danish Business Authority, some by the Danish Tax Agency, some by the Danish Agency for Digitisation, some by the police, some by Udbetaling Danmark etc. As many other relevant data are held by banks, it is obvious that expanded use of existing data could improve the efficiency of AML/CTF measures.

The case for expanding the collaboration between authorities and banks is therefore strong. First and

foremost, this will require more knowledge of which AML-relevant data are held where. Such knowledge will be relevant to authorities and banks alike. In addition, expanded collaboration will require some level of data sharing. This is a sensitive area, and it is important that due consideration is given to the protection of personal data and the duty of confidentiality of authorities and banks. For both banks and public authorities, the line between personal data protection and the general aim of combatting crime is a fine and sensitive one.

However, the general dilemma should not overshadow any legitimate concrete solutions that take into account the type of information to be exchanged, how important sharing the information is to the fight against crime, and how best to ensure the necessary protection of customers and their personal data.

Where the nature of the crime is concerned, it is relevant whether the case concerns big fish or little fish. In case of terrorist financing or money laundering involving very serious crime, such as human trafficking, drug empires etc, data sharing must be expected to be generally accepted as part of the efforts to catch the criminals. The same probably applies to other types of serious crime, for instance corruption. In other words: Big fish warrant general data sharing.

In relation to little fish, the dilemma is of another nature. In case of undeclared work or social fraud, more extensive data sharing would definitely improve AML efforts. Whether to allow this is primarily a political choice. Banks are faced with an almost impossible task of balancing interests in this difficult area, and a clear political stance is called for. There is a need for political and

perhaps public debate about where to draw the line in this context. More efficient combatting of undeclared work and social fraud could reduce economic costs in terms of a loss of tax revenues and unjustified benefits. The length to which public authorities and banks should go in this respect requires political debate, focusing on inherent dilemmas and the degree of determination to detect undeclared work and social fraud in order to obtain a clear political stance.

Where the protection of customers and their data is concerned, an important factor will be the nature of the data. As the data will mainly be of a financial nature, they are usually not deemed to be sensitive personal data. The consequences of being rejected as a customer may be significant, however.

Being rejected as a customer due to a suspicion of terrorist financing or serious money laundering will have serious consequences. Even though banks carry out thorough investigations, these investigations cannot be exhaustive. They have to notify the Danish FIU, which will carry out such exhaustive investigations. It is therefore possible that banks legitimately reject customers based on their ability to investigate suspected money laundering, but that more in-depth investigation proves such rejection to be illegitimate. Such "false positive" results have serious consequences for a customer. This applies despite the duty of confidentiality and even though the customer is not convicted but "only" rejected as a customer or reported to the Danish FIU. This dilemma already exists and will grow as more information is exchanged.

In this context the Task Force recommends that these

The Danish Financial Business Act

- Section 117[1] of the Danish Financial Business Act imposes on banks and their staff a duty of confidentiality; they may not without due cause disclose or use confidential information obtained, including all information about specific customers.
- Legitimate disclosure or use requires clear sta-

tutory authority or the customer's consent, must be customary (eg disclosure of credit information) or must be deemed legitimate based on a specific assessment. Whether disclosing information for the purpose of combatting money laundering, terrorist financing or other types of crime is legitimate will be subject to a case-by-case assessment.

dilemmas be discussed, and that, balancing the nature of the information and the nature of the crime, considerations are made as to how to optimise collaboration in general, including the general exchange of information, and to the possibilities of exchanging information in concrete cases. The latter in particular is very limited today, which makes AML/CTF initiatives far less efficient than they could be.

Collaboration forums

The Task Force finds it helpful that a number of collaboration forums have been set up to improve information about underlying crime, experience sharing and coordination.

The figure below shows the forums looked at by the Task Force in relation to collaboration with authorities. Recommendations on the individual forums are described below the figure.

Recommendations on general collaboration

Denmark has already set up or planned a number of forums for the exchange of information, especially on the crime underlying attempted money laundering and terrorist financing. The government's anti-money laundering and counter-terrorist financing strategy from September 2018 operates with the AML Forum for authorities and the AML Forum+ for authorities and relevant private-sector representatives. The aim of the AML Forum+ is to ensure the exchange between authorities and the private sector of information about general AML trends. The quarterly reports of the Danish FIU about AML trends are also an important instrument in that respect.

In addition, Finance Denmark has increased collaboration with the authorities based mainly on quarterly meetings offering an opportunity for the sector and relevant authorities to talk about general trends and developments in the area.

As mentioned earlier in this report, many stakeholders (private as well as public) and several legislations are involved in the efforts to combat money laundering and terrorist financing. This poses a challenge in terms of ensuring a coherent and coordinated approach across operators and legislative frameworks.

The Task Force therefore emphasises that increased coordination and collaboration between the relevant authorities in the area is key to the effectiveness of authority measures. The government's strategy in this area and the AML Forum are both important steps in the right direction.

In this context, the Task Force recommends that the Danish AML Forum should not only support the sharing of knowledge and experience but also serve to ensure a truly holistic approach across authorities in the form of, for instance, common supervisory priorities.

The AML Forum+ invites relevant AML authorities and trade organisations representing companies within the scope of the AML Act. At the AML Forum+ meetings, participants can share general knowledge, not comprising sensitive personal data or specific cases.

The Danish AML Act

- Section 38 of the Danish AML Act prescribes a special duty of confidentiality for banks, which are obliged to keep secret:
- 1) that a report has been submitted to the Danish FIU, 2) that the submission of a report is being considered, 3) that an investigation has been launched or 4) that an investigation will be launched.
- However, banks can disclose to other undertakings subject to the Danish AML Act that 1) a report has been submitted or submission of a report is being considered and 2) that an investigation has been or will be launched. A condition is that 1) the information relates to the same customer and the same transaction, 2) the recipient of the information is subject to AML/CTF requirements and 3) the recipient is subject to duties of confidentiality and protection of personal data.
- In practice, this means that the right to exchange data between banks is restricted to cases where the customer and the transaction are the same.

AML Forum

- The AML Forum was set up in pursuance of section 74 of the Danish AML Act and comprises a number of authorities involved in the fight against money laundering and terrorist financing. The objectives of the AML Forum include:
 - ensuring efficient and constructive inter-authority collaboration on combatting money laundering and terrorist financing

- ensuring coordination and exchange of information between authorities.

- The AML Forum will strengthen authority measures. Moreover, it will support the implementation of national and international obligations and assess the effectiveness of measures launched.¹⁸.

AML Forum+

- The AML Forum+ was set up as part of the Danish national strategy to combat money laundering and terrorist financing 2018-2021. The forum is hosted by the Danish FSA and offers private participants the opportunity to share issues and experience with authorities participating in the AML Forum. Finance Denmark participates in the AML Forum+.¹⁹

Forums in the AML area

For authorities only	For authorities as well as the private sector
<p>AML Forum</p> <ul style="list-style-type: none"> - Collaboration between authorities. 	<p>AML Forum +</p> <ul style="list-style-type: none"> - General exchange of information about overall trends - The forum is headed by the Danish FSA.
<p>Operational forum of authorities</p> <ul style="list-style-type: none"> - Collaboration between authorities. 	<p>Bank Forum</p> <ul style="list-style-type: none"> - General exchange of information between authorities and the members of Finance Denmark. - The forum is headed by the Danish FSA.
	<p>Joint AML/CTF Intelligence Unit</p> <ul style="list-style-type: none"> - Operational collaboration between authorities and selected bank members on specific cases. - Confidential forum headed by the authorities.

The forums in grey shade have already been set up, while the forums in turquoise shade are to be considered.

¹⁸ Source: Danish national strategy to combat money laundering and terrorist financing 2018-2021
¹⁹ Source: Danish national strategy to combat money laundering and terrorist financing 2018-2021.

The Task Force views the establishment of the AML Forum+ as an important measure to support the exchange of knowledge and best practice across sectors. It is important to keep in mind, however, that the participants are very diverse and have different levels of AML/CTF exposure. Therefore, there will still be a need for sector-specific forums where each sector, together with the authorities, can take deep dives into the challenges applying to that particular sector.

The Task Force further recommends that the Danish Data Protection Agency play a greater role in the AML Forum and the AML Forum+. Many of the challenges, and not least opportunities, in relation to improving efforts also involve data protection legislation issues. It is further recommended that the Danish Agency for Digitisation and perhaps Udbetaling Danmark be involved.

Banking Forum

In this context, the Task Force recommends the establishment of a banking forum for the financial area, giving authorities and the sector the opportunity to consider sector trends in depth and utilising the information available from authorities to improve banks' efforts to prevent and combat money laundering and terrorist financing. Such a public/private partnership could significantly improve the effectiveness of AML/CTF initiatives.

A Banking Forum would provide an opportunity to work in more detail with reports from banks to the Danish FIU, thereby increasing standardisation and qualification for the benefit of the Danish FIU's analytical processes and collaboration with the police, the tax authorities etc. The Forum would also be able to address training issues. Moreover, participants would be able to share experience concerning the risk of "false positives", issues with the duty of providing motivated rejections, the risk of tipping off criminals as well as opportunities and challenges of any additional data sharing. Specific discussions between participants could ease the dilemmas faced by banks (as described in the section "Dilemmas"). This would ensure a more harmonised practice and enable participants to strike the right balance where legislative frameworks overlap or give rise to doubt about suspicions. This forum would also provide an opportunity to discuss the alignment between the Danish AML Act and data protection legislation with the participation of the Danish Data Protection Agency and the Ministry of Justice.

Quarterly report and feedback from the Danish Financial Intelligence Unit on suspicions received

The Danish FIU prepares quarterly reports of the development in suspicions reported and in particular focus areas. These reports constitute a valuable tool for banks for organising their efforts.

However, the Task Force recommends that the Danish FIU look at ways to improve feedback on suspicions reported by the financial sector to the authorities. The legislation provides for the Danish FIU to give feedback on specific suspicions reported. The Task Force calls on the Danish FIU to make more use of such access. With more than 30,000 suspicions reported each year (a number likely to increase over the next years), this is obviously also a matter of resources. As an alternative, the Task Force therefore recommends that the Danish FIU look at ways to expand the quarterly reports.

Recommendations of increased collaboration in specific cases

The possibilities of exchanging information and experience in connection with specific cases are very limited today, which makes efforts in the area less effective. The FATF and the European Commission both call for more effective measures to combat money laundering and terrorist financing, to be achieved through coordination and exchange of information about specific cases and about the criminals exploiting the financial system.

The Task Force has been inspired by the relevant partnership between UK authorities and the UK financial sector.

Danish context

As mentioned above, Denmark has already set up or planned a number of forums for the exchange of information. However, an operational working group similar to the UK JMLIT has not been set up in Denmark. It appears from the Danish national risk strategy that the need to set up a permanent working group to discuss specific investigations with selected private participants should be considered. In connection with the political agreements concluded in autumn 2018 and March 2019, it was assumed that the framework for collective efforts to combat money laundering and terrorist financing would be improved.



In the opinion of the Task Force, the exchange of information about specific cases is required to be able to combat money laundering and terrorist financing effectively. A permanent, confidential working group could be a way to facilitate this and to address some of the concerns raised about increased information sharing.

A proposal for a Danish equivalent was presented at the Task Force's conference on 28 August 2019. The idea was welcomed by the politicians attending – who emphasised the importance of personal data protection, however. At a subsequent meeting with the Danish Data Protection Agency, it was concluded that such a solution would not seem to imply legal issues in terms of data protection.

Danish JMLIT equivalent: Joint AML/CTF Intelligence Unit

The Task Force therefore finds that such an operational unit should be set up; a unit which the Task Force proposes be called the Joint AML/CTF Intelligence Unit [“Den fælles Efterretningsenhed for Hvidvask og Terrorfinansiering”].

The Task Force is of the opinion that, like the UK JMLIT, the Joint AML/CTF Intelligence Unit should be set up within the public sector, with relevant participants from the State Prosecutor for Serious Economic and International Crime, the Danish FIU, the police, the Danish Tax Agency, the Danish Security and Intelligence Service, perhaps the Danish Defence Intelligence Service, and

representatives from the financial sector. The sector will select representatives from a number of banks. The representation should correspond to the membership composition of Finance Denmark. A possible model is that the composition could largely correspond to the composition of Finance Denmark's legal committee and that LOPI appoints representatives from the small banks.

To ensure personal data protection, the meetings of the working group should be confidential, and participants should have security clearance. This would be a condition for the exchange of classified information. Restricting the exchange of confidential information to a confidential forum where participants are subject to a duty of confidentiality would pave the way for easing the otherwise rather restrictive legislation in the area. Corresponding requirements must apply to the documentation, as there can be no doubt as to what is addressed in the confidential forum.

The main challenge of transposing the UK JMLIT model and especially its operational working group to Denmark is the rather limited right under Danish legislation to exchange information within the financial sector. This applies in particular to the Danish Financial Business Act and the Danish AML Act, as described in more detail above. It is therefore important that a clear legal basis be provided for a forum involving the same type of information sharing as the UK JMLIT.

The Danish government intends to set up an operational forum with the participation of the State Prosecutor for Serious Economic and International Crime, the Danish FIU, the Danish Security and Intelligence Service, the National Police, the Danish FSA, the Danish Business Authority, the Danish Tax Agency and the Danish Gambling Authority to strengthen the collaboration between authorities to combat money laundering and terrorist financing. In this operational group, the authorities will be able to present their knowledge of persons or transfers suspected of money laundering or terrorist financing.

JMLIT (Joint Money Laundering Intelligence Taskforce)

In the UK, the collaboration between authorities and the financial sector takes place in a public/private partnership. The aim is to prevent and combat money laundering, terrorist financing and financial crime through efficient collaboration. Focus is on collaborating on the exchange of information and research concerning money laundering, terrorist financing and financial crime. Collaboration takes place at both a strategic and a tactical level.

- Through an Expert Working Group, exchanging knowledge and expertise for the purpose of understanding the background, methods and threats of money laundering and terrorist financing. This is used to develop "alert" and "red flag" typologies for the purpose of identifying mitigating measures to prevent criminals from exploiting the financial system.
- Through an Operational Working Group where representatives from authorities and the financial sector meet every week in a confidential forum to exchange and discuss intelligence relating to specific cases.
- The exchange of information in the Operational Working Group is authorised by section 7 of the Crime and Courts Act 2013, and the JMLIT is regulated in detail by an agreement between the authorities and the financial sector.
- Similar arrangements have been or are being introduced elsewhere in the EU, including in the Netherlands, Ireland and Germany. The JMLIT has been pointed out as an example of best practice by, for instance, the FATF.



Solution model – proposed legislative amendment

The Task Force recommends the introduction of a separate provision in the Danish AML Act allowing the authorities, within the framework of the General Data Protection Regulation and the Danish Financial Business Act, to set up a working group for exchanging confidential information. The system seems to be working well in the UK; the solution is also recommended by the global organisation FATF and has attracted the interest of a number of other countries, eg Germany. It should therefore be possible, also in a Danish context, to establish appropriate measures to ensure data protection, confidentiality and compliance with documentation requirements, considering that the system will mainly be targeting the “big fish” at the upper end of the money laundering scale.

Introduction of a Danish Joint AML/CTF Intelligence Unit would support the main view that the corporate responsibility of banks in terms of preventing and combatting money laundering and terrorist financing should award banks the same access to knowledge sharing as authorities undertaking the same tasks. The social obligation calls for appropriate legal tools.

The financial sector's online AML/CTF training programme

- Trains staff and management of banks and other financial undertakings in anti-money laundering legislation and relevant guidelines.
- The programme was developed with the assistance of experts in the field.
- The programme is an online solution comprising e-learning and multiple-choice tests.
- The programme is adaptable to the job functions of individual staff members or staff groups.
- The undertaking can receive reports of programme results, enabling it to check that all staff pass the programme courses and tests.
- The training programme is regularly updated to reflect new legislation, guidelines etc in the area.

MAIN TRACK 3:

TRAINING

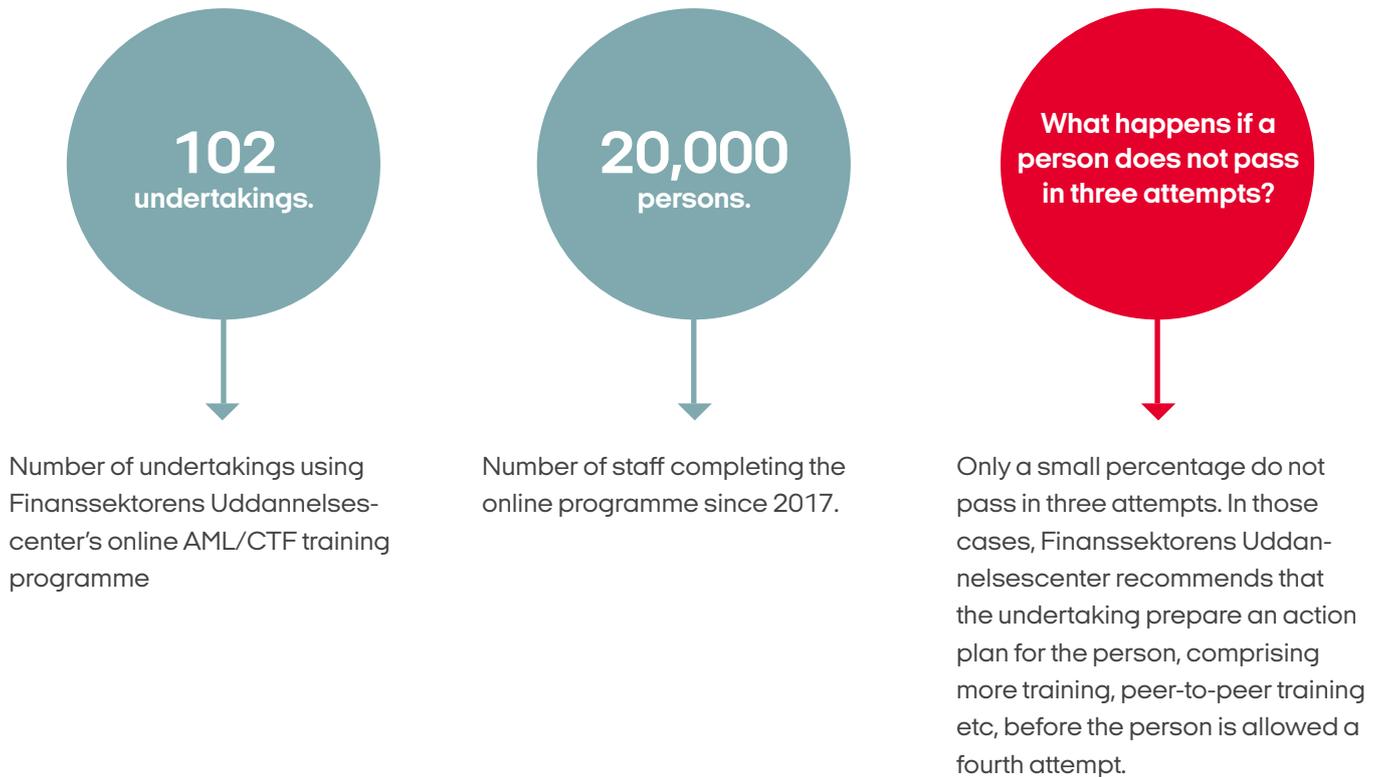
Banks must ensure that all members of staff and management are adequately trained in AML legislation and relevant data protection requirements²⁰. The requirement of adequate training implies refresher training at appropriate intervals²¹. Most Danish banks today use

the services of the Finanssektorens Uddannelsescen-ter (the financial sector's training centre), which offers an AML/CTF training programme. Danske Bank and Nordea have developed their own AML/CTF training programmes.

²⁰ Source: section 8(6) of the Danish AML Act.

²¹ Source: paragraph 7 of the Danish FSA's guidelines on the Danish AML Act [in Danish only].

Statistics and status at 14 August 2019²²:



Nordea's AML/CTF training programme

Nordea has divided its training programme into three categories:

- General training, function-specific training and external certification.

The general training course is mandatory for all Nordea's staff, approximately 30,000 persons. The course takes an hour and must be repeated every year. The course must be passed for the staff member to obtain a "licence to work". The course includes the following elements:

- Know Your Customer
- Anti-money laundering
- Counter-terrorist financing
- Compliance with international sanctions
- Prevention of bribery and corruption
- Prevention of tax evasion.

- Function-specific training must be completed by all customer-facing staff or staff working with AML/CTF, approximately 13,000 persons. In addition, staff with specialist functions involving the financial crime area receive ongoing mandatory training in their respective fields.
- External certification is provided by the International Compliance Association [ICA] to staff working full-time with financial crime prevention. As at end-2019, about 465 persons have completed an external certification programme. The programme duration is 3 to 9 months.

²² Kilde: Data fra Finanssektorens Uddannelsescenter

Danske Bank's AML/CTF training programme

- All Danske Bank staff complete a basic AML/CTF module.
- Danske Bank's training programme provides insight into why anti-money laundering and counter-terrorist financing are important to the individual, to society and to Danske Bank.
- The basic module is supplemented with different additional modules tailored to the functions of the individual staff members, such as customer onboarding, sanctions, monitoring and transactions as well as correspondent relationships.
- The function-specific modules provide an insight into the types of conduct to be particularly aware of in the individual areas.
- All modules are designed to train staff in the legal requirements while at the same time providing examples, cases and instructions tailored to Danske Bank's processes and frameworks.
- The modules are regularly updated to reflect new legislation, risk indicators and developments in the area.
- Danske Bank also has specialised programmes and peer-to-peer training aimed at staff dealing with customer due diligence in connection with onboarding and regular updating of customer due diligence data.
- In addition, Danske Bank uses an internationally certified AML/CTF training programme.



International ICA training

The International Compliance Association [ICA] is an international provider of training and certification programmes in the fields of compliance and regulatory prevention of financial crime. The ICA offers a wide variety of training programmes/certifications in, for instance, anti-money laundering, counter-terrorist financing, financial crime prevention, anti-corruption, the customer due diligence rules of anti-money laundering legislation etc.

Proposal – expansion

The Task Force has discussed the area of training and the training provided today. It is essential that AML/CTF training focuses the rules of AML legislation, but also that it can be tailored to the specific sector and not least to the individual bank. The staff should understand the overall risk and the message of the law, and also how the law is complied with by the specific undertaking based on its business model and in the specific job function of the relevant staff member. Each bank must always ensure that its staff are adequately trained in the bank's specific anti-money laundering and counter-terrorist financing measures.

Further case-based training and experience sharing

The Task Force considers the training provided today to be broad-based, but there is potential for further expansion and improvement, for instance by supplementing the existing training with more practical examples or cases. This would increase the understanding of concrete dilemmas, experience could be exchanged based on concrete situations, and the explanation of rules could be supplemented with a more practical approach.

Reports to the Danish FIU could be included as a natural part of the training and experience sharing exercise. This would enable a higher degree of qualification, standardisation and expansion of reports to make them as fit for purpose as possible. Standardisation would also support the research activities of the Danish FIU.

Sector solutions

It is also possible to increase collaboration and enhance training across the sector by drawing on the sector's collective practical experience. Cases could be developed that illustrate fraudulent chains, social fraud and other similar scenarios that fall within the concept of money laundering or terrorist financing. Such cases would also make the concepts of money laundering and terrorist financing more comprehensible to the staff.

The Task Force recommends that AML officers be offered training programmes that include experience sharing, case work and dilemmas. This would ensure a focus on the many concrete decisions to be made in connection with customer due diligence, onboarding and offboarding, risk scoring, criteria of transaction monitoring etc. For this purpose it is recommended that Finance Denmark hold biannual conferences, providing an opportunity to share experience in the area. This will promote uniform behaviour in the sector in practice.

Certification?

In this context, the Task Force has discussed the possibility of introducing an actual certification. The conclusion was that an actual certification would not be a flexible solution, as it would not allow the same degree of adaptation to a specific business model or bank-specific conditions. Also, it is important that training programmes are regularly updated to reflect new rules and experience in the sector, making ongoing training necessary and a one-off certification less suitable. An actual certification requirement is not deemed to be in the spirit of the law where focus is on management and staff understanding their business model and so-called inherent risk resulting from the geography, customer types, products and services, business partners etc of a business model. Furthermore, a certification solution would not in the same way as training meet the need for a continuous and flexible solution that will train the staff in case of changes in legislation, national risk assessments, the bank's own business procedures etc.

MAIN TRACK 4:

PRINCIPLES OF CONDUCT

Anti-money laundering regulation is exceptionally intense. It includes requirements regarding AML policies, the organisation of AML efforts, appointment of an AML Responsible Officer etc. Also, sanctions have been tightened substantially several times. Even though legislation, guidelines, EU Directives, EBA principles etc in the field of anti-money laundering are highly detailed, the practical implementation of the rules gives rise to many dilemmas and choices. The conduct of the individual banks varies greatly, as dilemmas and choices are addressed differently by different banks. They have different cultures and approach their tasks differently. All based on legislation – but also on their own systems, training programmes and focus. Against that background, the Task Force has developed a set of common principles of conduct in the field of anti-money laundering and counter-terrorist financing designed to align cultures across the sector.

Why are common principles of conduct beneficial?

The aim is to improve AML/CTF efforts and to ensure an ambitious commitment. For this purpose, all members of Finance Denmark must adhere to uniform principles, also supporting the view that AML/CTF efforts should not be a parameter of competition but a collective commitment based on common standards of conduct. Common principles of conduct will also serve to render visible any changes and to increase the transparency of banks' AML/CTF efforts. Finally, the Task Force considers common principles of conduct and a common culture to be a key condition for increased cross-sector collaboration and for the implementation of the Task Force's recommendations in respect of the other main tracks.

The Task Force has been inspired by similar codes of conduct or guidelines in other countries. The Netherlands, for instance, has had a significant focus on guidelines.



The Netherlands: The Dutch Banking Association [NVB] has developed an oath for persons employed in the Dutch banking sector. This "Bankers' Oath" provides the following guidelines:

Oath and discipline

Along with the introduction of a social charter and updating the Banking Code, the Dutch banking industry has also taken the initiative to implement an ethics statement (see annex). The Dutch banks intend this to show that everyone working in the industry is bound by the codes of conduct attaching to this statement for the ethical and careful practice of his/her profession. Employees have personal responsibility for complying with those codes of conduct and can be held accountable for non-compliance.

Since early 2013, policymakers and supervisors of financial institutions have by law had to sign the ethics statement, now better known as the bankers' oath. The initiative to have all bank employees take the oath will be a significant tool in creating the new culture wanted in the banking industry. A form of disciplinary scheme will be introduced to ensure that taking the oath is not without meaning. Bank employees will, therefore, be accountable to society as a whole.

Bankers' Oath

Form for the oath/affirmation by an employee other than a director or member of a body charged with supervision of policy and the general affairs of the business.*

I swear/promise that within the limits of the position I hold at any time in the banking industry:

- I will execute my function ethically and with care;
- I will draw a careful balance between the interests of all parties associated with the business, being the customers, shareholders, employees and the society in which the business operates;
- when drawing that balance, I will make the customers' interests central;
- I will comply with the laws, regulations and codes of conduct that apply to me;
- I will keep confidential that which has been entrusted to me;
- I will not abuse my knowledge;
- I will act openly and accountably and I know my responsibility to society;
- I will make every effort to retain and improve trust in the financial sector.

So help me God/This I declare and promise.

The oath/affirmation was taken/made in the above form on [date], at [place], before [name of person who administered the oath] in the presence of [name of other representative of the business or industry or professional organisation].

Furthermore, [name of the person] confirmed his/her acceptance of the enforcement of the codes of conduct by the Disciplinary Committee and the exercise of authority by the Director General pursuant to the disciplinary scheme in the banking industry codes of conduct.

Name [signature]

* The final text will be brought into line with the text of the Dutch Financial Supervision Act



The Danish FSA has now made it a requirement to have a policy for sound corporate culture. The requirement is a result of the political agreement of 19 September 2018. The obligation to have a policy for sound corporate culture applies to banks, e-banking providers and payment service providers. The policy must be adopted by the organisation's board of directors and must set expectations applying to all staff of how to behave and actively contribute to preventing money laundering and other financial crime etc. The Danish FSA will incorporate detailed policy requirements into an executive order²³.

However, it is essential that the principles of conduct are in step with the culture of Danish banks, and the Task Force has therefore decided to design the principles to fundamentally reflect the Danish conditions.

The main focus is on everyday behaviour, including banks' culture with respect to their corporate responsibility commitment. This aligns naturally with the Danish FSA's increased focus on a sound corporate culture.

Banks' tasks are mainly of a financial and advisory nature, with the focus being on returns, interest rates, investment, costs etc. However, over the past few years, the financial agenda has been supplemented with social obligations and corporate responsibility in terms of anti-money laundering and counter-terrorist financing. Sustainability, societal responsibility etc are other areas that are becoming ever more important. This prompts a natural need for a cultural alignment, making corporate responsibility a more integrated and visible part of

banks' day-to-day activities. It would also seem natural for this to take place at sector level in order to ensure uniformity and a concerted approach rather than silo mentality and silo solutions.

As part of the aim to further develop banks' efforts to prevent and combat money laundering and terrorist financing, the Task Force has therefore laid down six principles of conduct. These principles are based on a number of fundamental positions on banks' AML/CTF efforts. These are stated in the introductory remarks. Accordingly, a main principle is presented in a headline. This is followed by a more detailed description of the consequences for banks' everyday behaviour and efforts to prevent money laundering and terrorist financing.

²³Source: Section 70a(5) of the Danish Financial Business Act and section 25a(5) of the Danish Payments Act.

PRINCIPLES FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING BY BANKS

- ✓ We commit to combatting financial crime in a loyal and responsible manner.
- ✓ We recognise that the prevention and combatting of money laundering and terrorist financing is not a competition parameter and that collaboration and joint solutions are desirable.
- ✓ We will ensure that our management and staff adhere to these six principles and relevant instructions:

1. We always prioritise ethics over profit

- a. We prioritise anti-money laundering and counter-terrorist financing over profit and act according to the principle of no explanation, no defence.
- b. We only want customers with a clear and acceptable business purpose – and we stand firm whoever the customer.
- c. We insist on knowing our customers, their business and their use of a bank – even if it is met with opposition.

2. We comply with the spirit and the letter of the law

- a. We explain to our customers the background to the rules and the purpose of our efforts – comply and explain.
- b. We do our utmost to be an effective gatekeeper with respect to, for instance, high-risk countries, unusual transactions, complex or opaque corporate structures, large cash amounts etc.
- c. We do our utmost to be an effective gatekeeper with respect to undeclared work and social fraud, and we set up our systems accordingly.

3. We welcome oversight

- a. We recognise the need for increased transparency and find it important that our practice can stand the scrutiny of the public eye.
- b. In our management commentary, we will explain the main contents of our AML policy, and we will disclose information on our website about our specific efforts to combat financial crime.
- c. We will prepare standards based on common formats which can withstand independent review and form the basis for best practice.

4. We have a targeted corporate culture commitment

- a. We ensure that non-financial aspects are also considered when it comes to recruitment, promotion, remuneration etc, including that variable remuneration programmes comply with existing regulation.
- b. Our commitment to combat money laundering and terrorist financing is reflected in our day-to-day operations, our culture, our training programmes and our communication.
- c. We are inspired by other professions in our efforts to strengthen our culture and ensure that our commitment to combat money laundering and terrorist financing pervades all parts of our organisation.

5. We assume managerial responsibility and ensure that all staff take responsibility for AML/CTF efforts

- a. We set the tone from the organisational top as regards the communication and awareness of corporate responsibility, as managements are culture bearers.
- b. We ensure that all parts of the organisation continuously and very clearly emphasise the importance of our AML/CTF commitment – regardless of the tasks of the individual staff members.
- c. We provide relevant and adequate training of staff, qualifying them to perform their AML/CTF duties.

6. We have constructive partnerships with all stakeholders, including the authorities

- a. We target our reports to the Danish FIU so as to facilitate the most efficient fight against money laundering and terrorist financing.
- b. We participate constructively in the AML Forum+ and other collaboration forums that discuss the development in underlying crime and improve measures to combat money laundering and terrorist financing.
- c. We ensure access to effective, anonymous and protected whistle blowing.

Obviously, it is imperative that these principles are adhered to in practice. The Task Force therefore recommends that Finance Denmark support the sector's implementation of these principles.

MAIN TRACK 5:

INCREASED TRANSPARENCY

Besides the four main tracks, the Task Force has found that a particular focus on increasing the transparency of sector efforts is required. The Task Force has therefore decided to let increased transparency be a fifth main track.

Its work has prompted a number of recommendations as to how each bank individually and the sector collectively can raise the awareness of the public of the efforts and challenges in the area. The initiatives recommended by the Task Force are to be implemented at bank level and collectively at sector level through Finance Denmark.

Increased transparency in banks**Management commentary**

The Task Force recommends that the individual banks undertake to outline their anti-money laundering and counter-terrorist financing commitment, including their AML policy, in the management commentary of their annual reports. This goes beyond the obligations of the banks under the Danish Executive Order on Financial Reports for Credit Institutions and Investment Firms, etc.

Dedicated webpage

The Task Force also recommends that on their websites, banks dedicate a webpage to providing targeted and publicly available information about their anti-mo-

Banks with securities admitted to trading on a regulated market in an EU/EEA country must supplement their management commentary with a report on corporate responsibility. This report must provide information on the banks' CSR activities, including their corporate responsibility policy, how their policies are translated into action, what they have achieved and their expectations for the future²⁴.

In continuation of the corporate responsibility rules, the Task Force recommends that the individual bank outline its anti-money laundering and counter-terrorist financing commitment.

ney laundering and counter-terrorist financing efforts. Currently, the individual banks have different approaches to the nature of information provided. To make it easier for the public to understand banks' efforts, the Task Force therefore recommends that banks publish, as a minimum:

- A description of the bank's efforts to comply with Finance Denmark's principles of conduct in the AML area
- The main contents of the bank's AML policy
- The organisational setup/lines of defence of the bank in the area
- How customers are generally monitored
- How the staff is trained in the area
- A description of the bank's whistle-blower protection.

The above initiatives will raise the awareness of the public of the relevant measures of the individual banks, facilitating enhanced dialogue between a bank and its stakeholders. The information level should be measured so as not to provide criminals with too many details, enabling them to weaken the bank's lines of defence – but must provide enough details to increase transparency to the public.

Increased transparency in the sector through Finance Denmark

Annual conference

The Task Force recommends that Finance Denmark hold an annual conference thematising some of the challenges and dilemmas of financial crime. The conference should also provide an opportunity for dialogue with relevant stakeholders and with Finance Denmark's internal and external business partners.

Annual report

The Task Force recommends that Finance Denmark prepare an annual report with a detailed account of the sector's efforts in the area, including the development in reports made, allocation of resources, staff etc. The report should describe the risk areas faced by the sector, including the general types of cases in which reports

are made to the authorities. Finally, the report should describe new sector initiatives and standards from European neighbouring countries, and it should present proposals for increasing the effectiveness of AML/CTF partnerships between authorities and banks. This report should be shared with the public and be published at the annual conference.

Information to customers

The Task Force recommends that Finance Denmark provide more information to bank customers, explaining banks' efforts in the area and their obligations, including in relation to obtaining customer data and the purpose of this. This could be done through information campaigns, social media, pamphlets and direct (e)mail to bank customers.

Additional initiatives

Besides the five main tracks and relevant recommendations, the Task Force has considered a number of other measures to enhance the role of the sector in the fight against money laundering and terrorist financing. The Task Force has had a particular focus on specific initiatives to ensure knowledge sharing with the public, support research and strengthen collaboration between the sector and other organisations.

Against this background, the Task Force has come up with a number of sector initiatives.

Whistle-blower support

The Task Force recommends that the respective boards of directors – in addition to ensuring whistle-blower schemes in all banks – consider how to support whistle-blowers, for example by offering legal advice.

Collaboration with the State Prosecutor for Serious Economic and International Crime

The Task Force recommends that the sector, by way of the Joint AML/CTF Intelligence Unit, allocate staff for an exchange programme focusing on knowledge sharing for a period of up to three months.

²⁴ Source: section 135 of Danish Executive Order on Financial Reports for Credit Institutions and Investment Firms, etc.

Evaluation of reports made

The Task Force recommends that the sector, together with the Danish FIU, annually evaluate the reports made by banks to assure that they are of appropriate quality for the purpose of investigating suspicious activity and to avoid unnecessary reporting. An annual evaluation of sector reports could be facilitated by the new Joint AML/CTF Intelligence Unit.

Safe-deposit boxes

The Task Force recommends that the sector compile data on safe-deposit boxes. The reason for focusing on safe-deposit boxes is that they may be used to store criminal property, drugs, black money, etc. The sector should subsequently consider more closely how to establish a satisfactory level of preventive measures and processes when banks offer this service. In that context the Task Force recommends that the sector enter into a dialogue with the Danish FSA on industry guidelines with respect to effective monitoring of safe-deposit boxes as part of customer due diligence and monitoring requirements.

Proposals for future political initiatives

In its work, the Task Force has focused on the sector's own business procedures, systems and challenges and consequently solutions addressing these challenges. At the same time, the Task Force has discussed which initiatives could be launched, not only by the sector, but also politically. This chapter will present a number of proposals for future political initiatives.

Expanded collaboration between sector and authorities

It is important that the already strong relationships between the sector and the authorities be used to develop new ways of sharing information and knowledge. This will enable the authorities to benefit from the expertise developed by banks in practice and as part of their AML compliance, and banks to benefit from the information held by a number of public authorities. Where sharing more information is possible and deemed helpful, efforts can be qualified and focused on high-risk areas.

Banking Forum under AML Forum+

It is proposed as a supplementary political initiative that, in addition to the AML Forum for authorities and the AML Forum+ for authorities and trade organisations, a Banking Forum focusing on banks be set up with representatives from Finance Denmark and its members. Such a forum would provide a platform for detailed and industry-specific mutual knowledge sharing as well as discussions about specific issues.

Joint AML/CTF Intelligence Unit

In relation to the aim of expanded collaboration, it is proposed that a legal basis be provided for the establishment in Denmark of a Joint AML/CTF Intelligence Unit [reference is made to this report's description of main track 2: stronger partnerships with authorities]. To create a forum, headed by the authorities, where all resources, expertise and collected data will be used most efficiently, a statutory basis for a Joint AML/CTF Intelligence Unit should be pursued politically.

EU+

The Task Force recommends that Finance Denmark work to ensure that future EU regulation will explicitly provide for the establishment by the member states of a body similar to the Danish Joint AML/CTF Intelligence Unit and for cross-border exchange of information between these national units.

Guidelines on Danish AML Act

The Danish FSA's guidelines on the Danish AML Act is an important tool providing a general framework and general expectations in relation to risk-based regulation. Therefore, we need a continued focus on providing up-to-date guidelines on the anti-money laundering legislation, supporting in particular those areas where AML and other legislation conflict, as well as additional specific guidelines on specific situations where legislative history provides little guidance. Also, there is a continued need for guidelines to undertakings on the trends and scenarios that indicate money laundering and, especially, terrorist financing. Terrorist financing is generally harder to detect, as legitimate funds may be used for illegal purposes. Undertakings therefore need to know which scenarios to be aware of in their monitoring of customers and transactions.



APPENDICES

Appendix 1: Political anti-money laundering measures

The area of prevention and combatting money laundering and terrorist financing has been, and still is, an area of particular political focus, in Denmark as well as in the EU.

Denmark

Recent years have seen the conclusion of a number of political agreements in Denmark to step up the fight against financial crime, money laundering and terrorist financing. The agreements supplement the rules of the EU Anti-Money Laundering Directives, largely implemented in Denmark through the Danish AML Act.

Political agreements to combat financial crime, money laundering and terrorist financing:

- Agreement on enhanced measures to prevent money laundering etc in the financial sector of 21 June 2017: See the agreement here [in Danish].
- Agreement on additional initiatives to strengthen anti-money laundering and counter-terrorist financing efforts of 19 September 2018: See the agreement here [in Danish].
- Agreement on enhanced measures to prevent financial crime of 27 March 2019: See the agreement here [in Danish].

The political agreements from 2017 to 2019 have led to, for instance, a national anti-money laundering strategy, higher fines, increased resources to the Danish FSA and the Danish FIU, stricter fit and proper requirements,

increased protection of whistle-blowers etc. Further, the latest agreement set the aim that Denmark should have one of the EU's toughest regulatory regimes in the area.

The political initiatives were mainly implemented through amendments to the Danish AML Act in 2018 and 2019²⁵. Finance Denmark supports these agreements and has provided constructive input to the design of all the agreements.

Most recently the government decided to set up an operational authority forum with the participation of the State Prosecutor for Serious Economic and International Crime, the Danish FIU, the Danish Security and Intelligence Service, the National Police, the Danish FSA, the Danish Business Authority, the Danish Tax Agency and the Danish Gambling Authority to strengthen the collaboration between authorities to combat money laundering and terrorist financing.

Finance Denmark finds it imperative that clear, but risk-based regulation govern the area which is in keeping up with the development in society and also in criminal environments and trends, which are continuously changing as it becomes ever more difficult to misuse the financial system. Finance Denmark supports the initiatives, many of which go hand in hand with the sector's own enhanced efforts. It is beneficial that more resources are allocated to the Danish FSA and not least the Danish FIU so they have the necessary resources and are able to follow up on banks' efforts.



Finance Denmark also contributes by, for instance, participating in the Danish FSA's work on the guidelines for the Danish AML Act and through intensified collaboration with the relevant authorities in the area with focus on good and constructive dialogue and knowledge sharing. Partnerships with authorities on future measures are described in detail below.

EU

The Danish AML rules mainly implement the EU Anti-Money Laundering Directives, as well as the special rules following from the political agreements.

The current EU Directive is the so-called Fourth Anti-Money Laundering Directive of 20 May 2015, as amended and tightened by the Fifth Anti-Money Laundering Directive of 30 May 2018. The amendments will be finally incorporated in the Danish AML Act by 10 January 2020.

As part of the efforts to combat money laundering and terrorist financing, the European Commission proposed on 12 September 2018 to strengthen the European Banking Authority's (EBA's) role at national as well as EU level. With this proposal, European supervision will be centralised at the EBA, and the EBA will play a greater role in issuing guidelines for member states, and in intervening in specific cases.

Finance Denmark is in favour of the initiative, as it may support the efforts of national authorities, ensuring more uniform standards across the EU. However, day-to-day supervision should be vested in the national authorities.

The EU is also considering whether the European anti-money laundering legal framework should be laid down in a Regulation rather than a Directive going forward. A Regulation differs in that it applies directly in the member states.

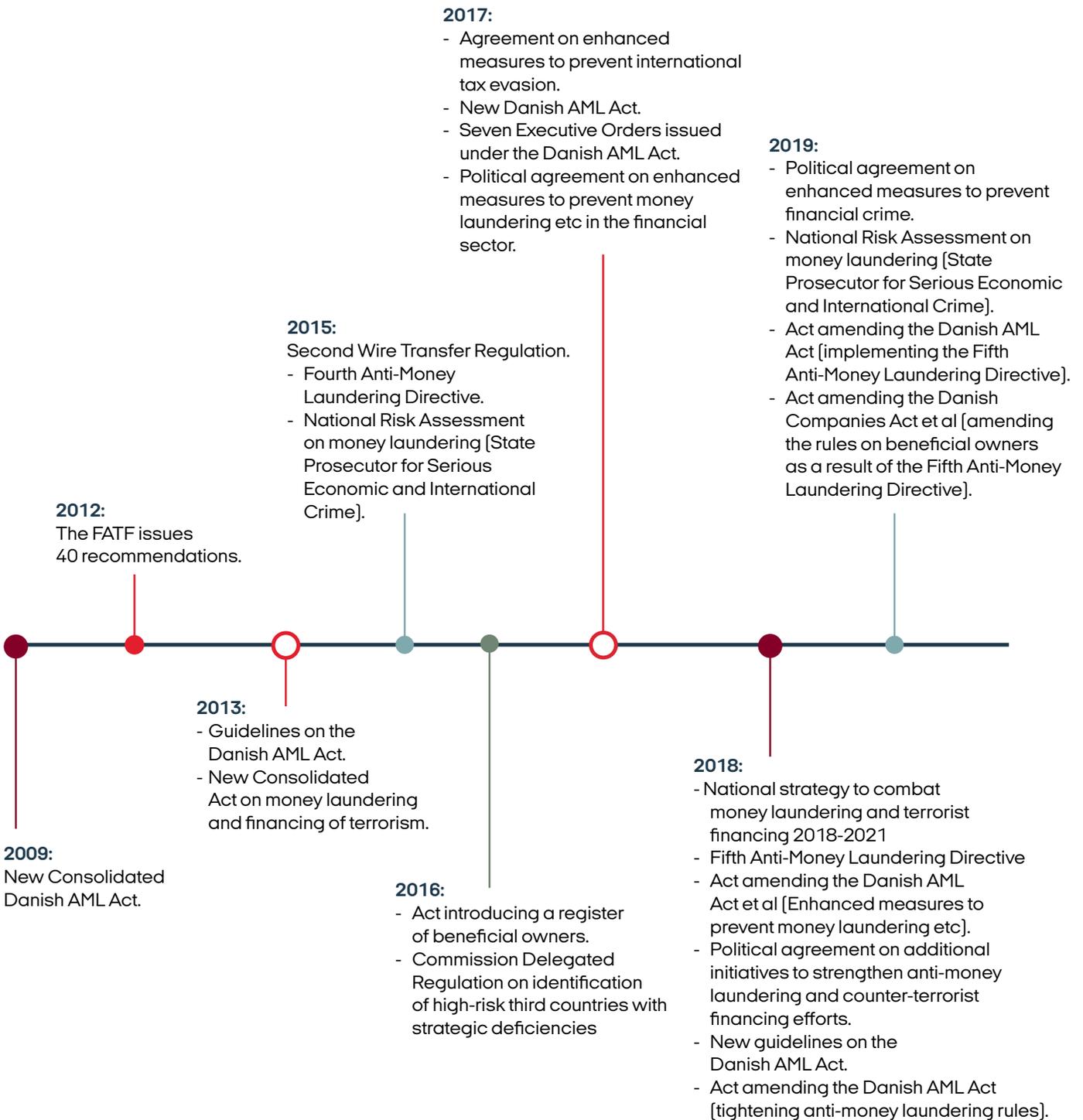
Both the Council and the European Parliament have recently asked the Commission to evaluate the area and consider whether the anti-money laundering legal framework should be laid down in a Regulation going forward, which the Commission seems to favour.

Against this background, the Commission published on 24 July 2019 one Communication and four reports reviewing the progress in addressing the regulatory and supervisory shortcomings believed to have been identified and making a number of recommendations for improvement.

Particularly relevant is the Commission's conclusion that banks and national supervisors have adopted essential measures, but that still more needs to be done. Further harmonisation is called for. Moreover, the Financial Intelligence Units (FIU) are emphasised – the Danish FIU is the Money Laundering Secretariat under the State Prosecutor for Serious Economic and International Crime. In the opinion of the Commission, the possibilities of collaboration and exchange of information between the FIUs are insufficient.

²⁵ Source: Act no 1535 of 18.12.2018, Act no 706 of 08.06.2018, Act no 533 of 07.05.2019.

Appendix Timeline – AML initiatives over the past 10 years





Grafisk design: Wundergeist.dk
Foto: Finans Danmark og Unsplash

Finance Denmark
Amaliegade 7
DK - 1256 København K

Phone: +45 3370 1000
www.finansdanmark.dk

