Dutch Banking Association

The case for further reform of the EU's AML framework

November 2019

Who are we? The Dutch Banking Association represents the Dutch Banking Industry. Our membership consists of different types of banks, ranging from highly specialised businesses, small and large Dutch lenders, as well as large international banks. All our members have a strong footprint in the Netherlands.

1. INTRODUCTION AND KEY RECOMMENDATIONS

As crucial gatekeepers, banks must play an important role in upholding the integrity of the banking system, a crucial element in the fight against financial crime and terrorist financing.
Maintaining this integrity is one of the key challenges our sector faces today, and this challenge can only be met by fostering a constructive dialogue with the public sector.

Former Dutch Finance Minister Dijsselbloem once called the financial crisis a 'blessing in disguise', referring to the significant steps made to make banks safer in its aftermath. We hope recent money-laundering incidents implicating several European banks will trigger a fundamental rethink of how we fight financial crime.

The financial crisis was the catalyst for the Eurozone's Banking Union. We believe the currently inadequate approach to fighting financial crime requires a strong European answer as well. Financial crime is a cross-border problem, which requires cross-border solutions both at European and global level.

The core of our EU policy recommendations, which are explained in detail in this paper, are:

1. *Harmonise the EU legal framework*
2. *Europeanise supervision and enforcement*
3. *Encourage better execution through facilitating cooperation between gatekeepers*

A key factor that determines the effectiveness of the joint fight against financial crime is public-private cooperation. It is important that the public and private sector fulfil their roles as gatekeepers of the financial system together.

Although we welcome recent additional efforts of EU and national policymakers to tackle financial crime, including granting further powers to the European Banking Authority, tweaking the rules at EU level and developing a national action plan in our Dutch home market, we believe more needs to be done.

The EU's new legislative mandate offers a window to holistically tackle this agenda through an EU wide response. The European Commission already provided highly valuable input into this process with its post-mortem assessment of the recent AML cases involving European bank, its supranational risk assessment, and its assessment of the framework for FIUs published in July 2019[1].

[1] European Commission, 24 July 2019:
https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en

Dutch Banking Association

Overview of Policy Recommendations

Effective EU rules

- Turn the lion's share of the EU AML Directives into an EU Regulation
- Limit national discretions in that EU Regulation to a bare minimum
    - Pay specific attention to access to the UBO register in this regard and ensure harmonised full access to data by obliged entities throughout the EU.
- Allow banks to rely on UBO data for KYC purposes for low-risk transactions
- Ensure the scope of entities designated as gate-keeper is technology neutral, in order to avoid regulatory gaps, particularly in light of the emergence of new technologies.
- Empower the European Data Protection Board (EDPB) and EBA to provide clear EU wide guidance on the interaction between EU privacy rules (notably GDPR) and AML techniques, with the specific goal of providing clarity to gatekeepers as to what is allowed in terms of information sharing.
- EU policy makers should write-in risk-based criteria for enhanced or simplified due diligence in the level 1 legislation, in order for the framework to remain risk-based as intended by the legislators.

Effective EU supervision and enforcement

- *EU policy makers should set up an independent EU AML supervisor, which would directly supervise the EU's most risky obliged entities.*
- *Low-risk entities could remain under the scope of the national AML supervisors, respecting the proportionality principle.*
- *EU policy makers should also consider setting up an EU-wide FIU, which would help overcome the challenges of international cooperation, help build expertise on cross-border crime, and enhance the EU's influence in the world.*
- If policy makers pursue a reform of Europol, financial crime with an EU dimension could be considered to become part of a strengthened EU law enforcement capability.
- Policy makers should investigate the potential for the European Public Prosecutor's Office to prosecute financial crime with an EU dimension.
- The EU should stimulate public-public cooperation agreements between stakeholders involved in fighting financial crime (including law enforcement).

Effective EU execution

- EU policy makers should encourage public-private partnerships to fight financial crime, and clarify the conditions for operational data sharing between actors
- EU law should explicitly allow certain forms of cooperation between gatekeepers where cooperation will improve the gatekeepers' effectiveness. This includes shared KYC and transaction monitoring utilities, as well as the development of "red flag" high risk clients.
- On top of encouraging cooperation agreements, EU law should also encourage stronger feedback loops between public and private gatekeepers.

These recommendations are outlined in detail in section 3 of this paper.

Dutch Banking Association

2. WHY DO WE NEED TO CHANGE THE WAY WE FIGHT FINANCIAL CRIME IN EUROPE?

Despite public authorities and the EU financial sector spending billions of Euros annually combatting financial crime[2], we must recognise that the results of these collective efforts have proven insufficient.

At the heart of the problem is that the way we fight financial crime in the EU has proven largely ineffective. Integration of financial systems, together with the rise of new innovative technologies, has resulted in further proliferation of financial crime.

For example, technology has made it easier to conceal the identity of ultimate beneficial owners, which is challenging law enforcement and financial institutions to detect and prevent suspicious transactions.

Despite these challenges, the banking sector needs to accept its responsibility, as it has sometimes failed to consistently play its role as a one of the key gatekeepers in this system, including because the actual results from banks' efforts have proven disappointing.

To complement efforts to address the shortcomings of the banking sector itself, we believe the effectiveness of gatekeepers could be enhanced by tackling shortcomings in the regulatory and supervisory design of the EU's AML framework and by tackling barriers that currently hinder cooperation between all parties involved.

We recognise that an effective framework to fight financial crime will continue to require significant investment from our sector and that we bear responsibility as a key gatekeeper in the financial system.

The banking sector should commit to taking on this challenge, as this is what regulators, clients, staff, shareholders, and the communities we serve expect from us.

In the below we outline our vision and propose concrete recommendations on how we believe the system can be improved.

What does a bank do to fight financial crime?

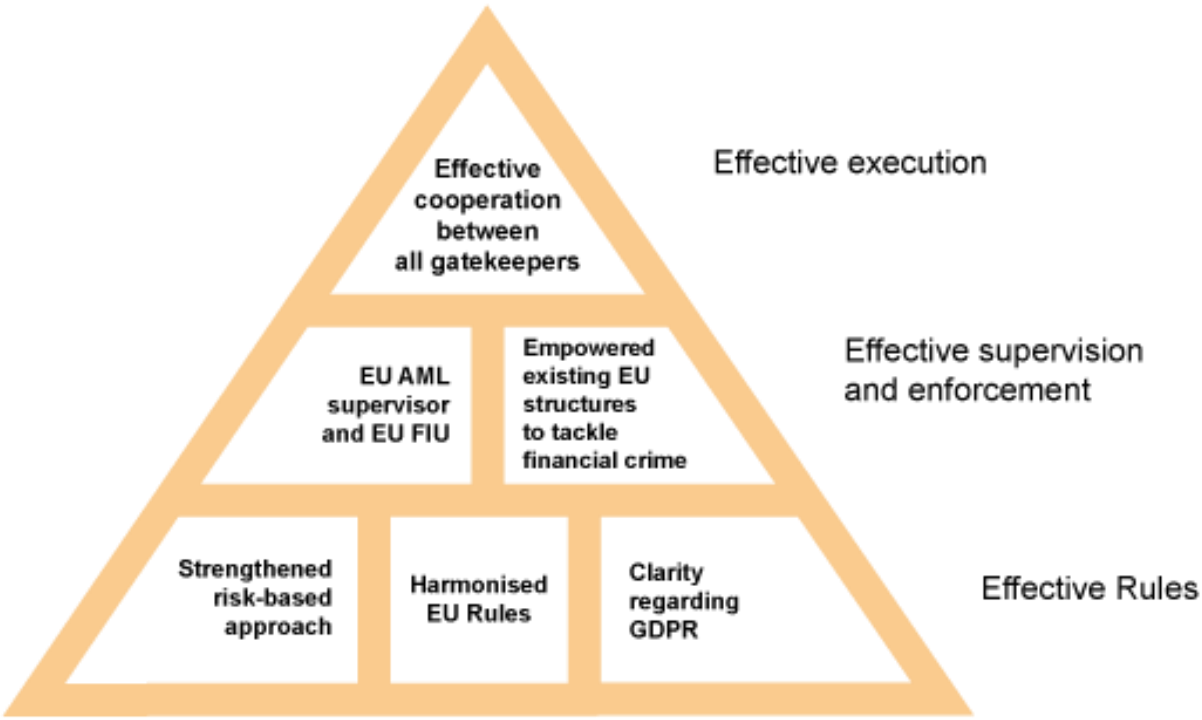
- ***Customer Due Diligence*** – Before onboarding a client, a bank checks who their new potential costumer is. Banks repeat this process periodically during the client relationship.
- ***Enhanced Customer Due Diligence*** – In certain circumstances, banks are required to apply enhanced checks, for example when dealing with entities in high-risk countries, politically exposed persons, or when a bank acts as a correspondent bank. Enhanced due diligence also applies when either a Member State or the European Commission assesses that a subset of transactions poses enhanced money laundering risk. This is determined by (supra-)national risk assessments.
- **Simplified Customer Due Diligence** – In certain circumstances, Member States can allow obliged entities to apply a simplified form of due diligence. This is linked to the judgement of the riskiness of a (set of) transactions, i.e. the inverse of how enhanced due diligence works.
- ***Transaction monitoring / suspicious transaction reporting*** – banks monitor client transactions and report suspicious activities to national Financial Intelligence Units (FIU).

[2] The European Banking sector is estimated to spend €20 billion annually combatting financial crime. See Politico interview with Rob Wainwright, 5 April 2018: https://www.politico.eu/article/europe-money-laundering-is-losing-the-fight-against-dirty-money-europol-crime-rob-wainwright/

Dutch Banking Association

3. HOW TO IMPROVE THE EU FRAMEWORK

Foundations for fighting financial crime in the EU



3.1. Effective rules

3.1.1. The EU's AML legal framework needs to be fully harmonised

Turn the AML Directives into a Regulation
Financial crime can be highly sophisticated, and it is entirely feasible to assume criminals are able to exploit regulatory inconsistencies and weaknesses between jurisdictions, even between EU Member States[3].

Currently, the AML rules are contained in EU Directives, which need to be transposed into national law. This has led to significant differences in interpretation of the EU framework in different Member States. We believe the lion's share of the provisions in the current Directives should be restructured into a directly applicable EU Regulations. Such approach would be a necessary step to build an EU 'maximum harmonisation' framework for AML.

This should certainly include rules on due diligence, transaction reporting, and record keeping, amongst other things.

[3] We recognise this problem is global in nature, and not restricted to the EU. However, we have chosen to focus on the intra-EU perspective in this paper.

Dutch Banking Association

Remove discretionary powers for Member State
At the same time, and sometimes because they are contained in Directives, the AML rules allow for significant Member State discretions, as the EU legislators have given Member States a high degree of freedom in choosing policy options.

These differences can provide criminals with an incentive to move activity to jurisdictions with the 'weakest' rules. The weakest jurisdiction then becomes the European Single Market's Achilles' heel.

We believe the EU's framework on AML should leave only very little discretion to Member States, and the EU rules should be characterised by the principle of maximum harmonisation, leaving optionality to Member States only in very defined instances where there is a clear justification that national specificities need to be taken into account.

In the current framework, examples of differences between jurisdictions range from:

- The definition of what certain offences mean in different jurisdictions
- How KYC/Customer Due Diligence requirements are applied
- Rules around filing suspicious activity reports (SARs) and the threshold to activate the SAR mechanism

Give obliged entities full access to reliable UBO registers

An important outstanding national option stemming from the 4th AML Directive is that Member States have some freedom in determining the level of access banks have to Universal Beneficial Ownership (UBO) registers[4]. This might indeed lead to discrepancy of access to this important information. As the Dutch Banking Association, we strongly believe obliged entities should have unrestricted access to UBO registers, as it would significantly improve gatekeepers' ability to effectively perform its tasks.

The other key element that will determine the usefulness of the UBO register is the quality of its data. Making data available will not suffice. Public authorities – in its role as gatekeeper - should implement their own systems to assess the quality of the data, and the banking sector should assist public authorities in their efforts, mainly through reporting discrepancies between what is contained in the registers and the banks' own due diligence data. This is a good example of public-private cooperation which we will discuss in detail in point 3.3.

Based on qualitative data, and only in cases where clients pose a low risk, we believe obliged entities should be able to rely on the information in the UBO to conduct KYC/CDD checks relying solely on the data from the UBO as "golden source" data. We believe this would in line the 4th AML Directive, and we would urge this principle will be applied in jurisdictions across the EU. A clear EU Regulation would provide more certainty in this regard.

Enhance technology neutrality

Harmonising the AML rules could also provide an opportunity to make the rulebook technology neutral. The current approach based on descriptively defining obliged entities can in principle lead to new technologies prone to AML risk falling between the cracks until primary legislation is adjusted.

A principle-based approach, where all entities engaged in financial transactions are covered unless they are specifically exempted, could be an avenue to consider in this regard. The second EU Payment

[4] Article 30(4) of 4AMLD) – "The persons or organisations referred to in point (c) shall access at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held."

Dutch Banking Association

Services Directive (PSD2), which regulates an area equally subject to rapid technological change, also uses this approach.

The recent proliferation of cryptocurrencies/stablecoins/virtual assets and related financial products (such as Initial Coin Offerings) are a good case in point here. While the EU's 5th AMLD captured wallet providers and providers of exchange services between cryptocurrencies and virtual currencies, The Financial Action Task Force's June 2019 Guidance goes further and recommends including other crypto-related services such as crypto-to-crypto exchanges and crypto issuers (i.e. those arranging ICOs).

We would certainly support this FATF guidance to be converted into EU law. However, with the current approach to the scope of the AMLD, it will take a few years at least for this to materialise in practice. This mechanism can allow serious risks of regulatory gap in times of rapid technological change.

Policy recommendations:

- *Turn the lion's share of the EU AML Directives into an EU Regulation*
- *Limit national discretions in that EU Regulation to a bare minimum*
- *Pay specific attention to access to the UBO register in this regard and ensure harmonised full access to data by obliged entities throughout the EU.*
- *Allow banks to rely on UBO data for KYC purposes for low-risk transactions*
- *Ensure the scope of entities designated as gate-keeper is technology neutral, in order to avoid regulatory gaps, particularly in light of the emergence of new technologies.*

3.1.2. Financial market participants need further legal clarity around the interactions between AML and personal data legislation

Since the EU's General Data Protection Regulation (GDPR) is in full force, questions have arisen from market participants around how certain provisions contained in the legislation – for example around the 'right to be forgotten' and 'consent' – apply to obliged entities under the EU's AMLD.

While we fully support the EU's strong approach to data privacy, we believe it would be beneficial in certain instances for financial market participants to be provided with EU-wide clarity about the interaction between GDPR and AML requirements.

For example, it remains unclear whether an obliged entity would have to comply with a person's request for them to delete data held (under the provision of the right to be forgotten under GDPR) – even if the person is convicted or suspected of money laundering.

Elsewhere, finding the right balance between GDPR and fighting financial crime is a key consideration when thinking about public-private and private-private partnerships, which have significant potential to fight financial crime more effectively. The Dutch government helpfully conducted an exercise to test

Dutch Banking Association

cooperation options against the GDPR (and other privacy laws) in the framework of the Dutch action plan against financial crime[5].

While we strongly welcome the push for clarity at national level, an EU-wide approach to this question could foster cross-border cooperation. The European Data Protection Board, the supervisory board established by the GDPR, should play a key role in this. This guidance on how to interpret the GDPR in an AML context could be developed in consultation with the European Banking Authority, to ensure the trade-off between data protection and AML enforcement is balanced.

The high fines linked to GDPR breaches make clarity even more important. While we certainly understand that the high fines are necessary to give the GDPR regime sharp teeth, it seems unavoidable that, faced with a lack of legal certainty, obliged entities will likely take a cautious approach (including at board level). In certain cases, this might hamper to most effective approach to fighting financial crime.

Policy recommendations:

- *Empower the European Data Protection Board (EDPB) and EBA to provide clear EU wide guidance on the interaction between EU privacy rules (notably GDPR) and AML techniques, with the specific goal of providing clarity to gatekeepers as to what is allowed in terms of information sharing.*

3.1.3. Strengthen the risk-based approach

The relatively small amount of laundered funds seized in Europe is often seen as a consequence of the model of compliance that has been adopted in the EU.

Because both supervisors and obliged entities often view AML rules through the prism of tick-box compliance – i.e. once the rules are 'technically' adhered to, their duties are considered fulfilled – discretion is hardly ever applied to the rules due predominantly to the already existing costs of compliance.

The knock-on impact of this approach is that it can lead to de-risking by banks, and other financial institutions, resulting in financial exclusion of certain cohorts of society and increased compliance costs for EU businesses, both large and small. For example, the European Association for Corporate Treasurers (EACT) estimated that large firms spend on average 25 hours a week responding to banks' KYC requests[6].

We believe a re-think about how to use best collective resources is required in this context.
Ideally, a proportionate and risk-based approach to AML assessments should be put forward, allowing the entire eco-system (obliged entities, FIUs, law enforcement, & AML supervisors) involved in AML prevention to collaborate and determine the types of transactions which should be considered risky. This would notably include obliged entities being able to share KYC utilities, and to allow certain forms of shared transaction monitoring. We discuss this in detail in point 3.3.

[5] "Onderzoek naar informatie uitwisseling", Dutch Government, 1 July 2019: https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/01/onderzoek-informatie-uitwisseling
[6] "EACT Briefing Focus: KYC", European Corporate Treasurers Association, 14 March 2019: https://www.eact.eu/news/118/eact-briefing-focus-kyc/

Dutch Banking Association

A key example of enhancing a risk-based approach could be the use of UBO data, which we highlighted in the previous chapter. To enhance the risk-based approach, obliged entities should be able to fully rely on UBO data for its CDD, unless there is a specific reason to believe the information in the UBO register is incorrect. This feeds into a wider point that EU legislation and other EU rules should clearly define the triggers where additional measures have to be taken, which will allow all gatekeepers (including public authorities) to focus their attention on high-risk cases (based on data) instead of unfruitfully trying to remove all risks from the system.

For example, we note that some supervisors today consider clients that are onboarded without face-to-face identification as high risk. It is unclear which risk trigger justifies this assessment.

This different philosophy would entail that, beyond the designated obliged entities, public entities such as the FIUs, law enforcement and AML supervisors, would consider themselves as part of the gate-keeping mechanism in the financial system, meaning they actively help the obliged entities in their due diligence tasks, notably through setting-up and participating in the relevant public-private partnerships.

To complement this, we would welcome the European Banking Authority providing further guidance around national and supranational risk assessments, which form the bases of enhanced due diligence requirements nationally and at EU level, particularly in order to clarify the level of discretion provided to national authorities.

Policy recommendations:

- *EU policy makers should write-in risk-based criteria for enhanced or simplified due diligence in the level 1 legislation, in order for the framework to remain risk-based as intended by the legislators.*

3.2. Effective supervision and enforcement

3.2.1. An EU AML supervisor and an EU Financial Intelligence Unit will reduce complexity and increase effectiveness

The case for direct EU supervision on certain obliged entities

To leverage the positive effects of maximum harmonisation of the AML rules, we would support the creation of a new European AML supervisory body that would directly supervise the riskiest obliged entities. This would not only strengthen enforcement but would also foster a common supervisory culture and good practices in the EU.

A new EU body seems needed as existing EU structures such as the ECB/SSM – whose coverage is restricted to the Eurozone and credit institutions; and the EBA, whose governance structure and its agency relationship with the European Commission could restrict its ability to act a supervisor - do not seem ideally placed to fulfil this task.

Dutch Banking Association

This new supervisor could be modelled after the SSM (but covering the entire EU), only directly supervising the most important financial sector obliged entities under its remit. To ensure proximity with local jurisdictions, EU direct supervision should be executed by Joint Supervisory Teams. The new EU body would also improve cooperation between existing national supervisors, acting as a *first among equals* of the EU's supervisory system.

Whether or not an institution would be directly supervised by the new EU AML supervisor would need to be determined by how risky the entity is. Participating in cross-border transactions would serve as one of the factors to assess riskiness. While size should be a factor as well, it should be recognised that the SSM approach should not be replicated, as the relationship between size and riskiness is less strong when it comes to AML.

We recognise the complex nature of determining ML risks would require a dynamic approach in determining where an EU supervisory body would directly intervene. We would however urge for a careful balance to be struck between being dynamic and maintaining a predictable supervisory environment for obliged entities.

The residual category of financial sector obliged entities, as well as most of the non-financial sector obliged entities could remain under the auspices of national AML supervisors, who - like in the SSM model - would continue to exist and perform important tasks. Although in many cases non-financial obliged entities would likely be considered less risky in the first place, it is worth investigating whether some of the large and risky non-financial entities could fall under the direct remit of an EU supervisor as well. As always in EU matters, it is important the proportionality principle is respected.

A single supervisor would also simplify the current framework, remove inefficiency from the system, including around exchange of information/coordination, and most importantly help prevent regulatory arbitrage. It would also allow real expertise to be developed within the institution and arm it with real credibility and accountability in AML.

An EU-wide Financial Intelligence Unit

We would support the creation of an EU Financial Intelligence Unit which could incorporate the existing Europol structure of FIU.net and replace the European Commission's FIU platform structure.

In line with the reasoning on supervision, an EU-wide FIU would reduce the risk of criminals exploiting weaknesses across jurisdictions, while it would also mirror the cross-border nature of financial crime.

An EU FIU would also give the EU a strong united voice in the international Egmont Group which brings together FIUs from around the world. This would strengthen the EU's ability to influence a debate that can be expected to become increasingly global.

The main function of an FIU is that it investigates suspicious activity reports ("SARs") that obliged entities are required to report to them. One possible set up of an EU FIU could be for it to focus on cross-border SARs and be able to delegate tasks to national FIUs. National FIUs could also call on the expertise of the EU FIU in cross-border cases.

The EU FIU would be able to build economies of scale and expertise around cross-border criminal activities and serve as the central nod in the system of existing FIUs. Although AMLD5 has provided for cooperation/information sharing requirements between FIUs, we believe an EU FIU would be able to add real value to the EU ecosystem. To improve operational efficiency, the EU FIU could be incorporated as a separately managed unit of the EU AML supervisor.

Dutch Banking Association

Policy recommendations:

- *EU policy makers should set up an independent EU AML supervisor, which would directly supervise the EU's most risky obliged entities.*
- *Low-risk entities could remain under the scope of the national AML supervisors, respecting the proportionality principle.*
- *EU policy makers should also consider setting up an EU-wide FIU, which would help overcome the challenges of international cooperation, help build expertise on cross-border crime, and enhance the EU's influence in the world.*

3.2.2. Empowering other EU institutions to fight financial crime jointly

Beyond the creation of new institutions that will help build unified supervision, other existing EU bodies could be strengthened in their AML function.

We recognise that this part of the ecosystem, linked to law enforcement, falls largely outside the remit of financial regulation, which is why we very much focus on some basic principles in this chapter.

We strongly support the role of Europol and Eurojust in promoting cooperation between law enforcement and prosecutors across EU jurisdictions. The Netherlands being plagued regularly by international crime, we are advocates for a strong European framework for law enforcement.

We take note of the recent calls – including from the European Parliament – to reform Europol into a stronger European agency with executive powers (the term "European FBI" has been used in this context). If such an idea were to be pursued, we believe financial crime should certainty be one of the top priorities as part of a mandate to tackle cross-border organised crime and terrorism, particularly in a cross-border context.

The set-up of the European Public Prosecutor's Office (EPPO) by 22 EU Member States is also a potential avenue to explore further in the context of AML. Although the initial focus of the EPPO will be on cross-border crime against the EU budget (i.e. fraud, corruption, or serious cross-border VAT fraud), European policy makers could consider exploring the potential for the EPPO to receive a mandate to prosecute financial crime with an EU dimension.

These are likely to be longer term projects. In the meantime, cooperation between authorities (including law enforcement) should be strengthened further. We believe the Dutch Financial Expertise Centre (FEC), which brings together all public sector stakeholders involved in fighting financial crime (*see below*) could be a good blueprint for similar cooperation agreements at EU level.
The Dutch Financial Expertise Centre is a collegial body that brings together supervision, control, prosecution, and investigation public authorities within the financial sector with the sole objective of fighting financial crime.

Dutch Banking Association

Policy recommendations:

- *If policy makers pursue a reform of Europol, financial crime with an EU dimension could be considered to become part of a strengthened EU law enforcement capability.*
- *Policy makers should investigate the potential for the European Public Prosecutor's Office to prosecute financial crime with an EU dimension.*
- *The EU should stimulate public-public cooperation agreements between stakeholders involved in fighting financial crime (including law enforcement).*

Dutch Banking Association

3.3. Effective execution

3.3.1. Better collaboration between public and private sector to fight financial crime

Better public-private and private-private cooperation is one of the most promising ways to improve the effectiveness of the EU AML framework.

The Dutch government, as part of a recent action plan on anti-money laundering, conducted a thorough analysis of different cooperation models, which we strongly supported as it has fostered an evidence-based debate on this issue. We would strongly recommend a similar exercise at EU level.

The Dutch government's exercise led to both a commitment to address certain legislative barriers to the cooperation models; and clarification that in some cases, no such barriers exist. We would welcome similar clarity at EU level, which could include legislative changes where necessary. This would include an analysis of the interaction of AML rules with the GDPR and competition rules.

That said, we believe the ground-rules for cooperation should always be:

- Gatekeepers (including banks) should never be able to outsource liability/responsibility
- A trade-off has to be made between increased effectiveness on the one hand and privacy concerns on the other. Proportionality is the key word.

TYPES OF COLLABORATION

Public-private partnership - partnerships like the Dutch "Serious Financial Crime Task Force[7]" – currently in pilot stage – where public and private gatekeepers share information, should be encouraged at the EU level. We realise this is challenging given the limited competence the EU has in this area, but a reform of Europol might serve as a good basis in this regard. The existing Europol Financial Intelligence PPP (EFIPPP) could also serve as a good basis.

We acknowlegde that sharing of non-personal, aggregated, data, should already be possible under the existing frameworks if strict conditions are met. Operational data sharing – which can include personal data – however, seems only possible in the framework of terrorism financing. The Dutch Serious Financial Crime Task Force will provide a framework to share operational data, which we welcome. We would welcome an EU framework to specify under which conditions operational data could be shared.

Shared KYC check capabilities ("KYC utility") – the EU framework should make explicitly clear that gatekeepers should be able to create joint KYC capacities under certain circumstances:

- Based on consent of the individual client
- In line with competition rules (notably the utility should not exclude new members from joining on a reasonable basis)

KYC utilities are not only useful tools for banks, they will bring about significant efficiency gains for our clients, given less time will be spend on responding to KYC requests (important for both individuals and businesses).

Shared Transaction Monitoring ("TM Utility") - criminals can easily do transactions using different banks. The only way for gatekeepers to see patterns in these transactions is to share data around transaction monitoring. The Dutch government has recognised national legislation currently impedes legitimate data sharing between banks and has committed to removing these impediments. The EU AML

[7] "Convenant Pilot Serious Crime Taskforce", Staatscourant, 6 August 2019: https://zoek.officielebekendmakingen.nl/stcrt-2019-43629.pdf

Dutch Banking Association

rules should clarify this issue at EU level, through maximum harmonisation, by explicitly allowing outsourcing of transaction monitoring under stringent conditions (notably that the gatekeeper does not outsource its liability/responsibility).

Identifying high risk clients – We would welcome being able to share amongst banks a list of clients with whom relationships have been terminated or where the client has been refused based on KYC due diligence. This list would serve for obliged entities to warn each other about risks and improve KYC checks significantly. The EU should clarify the relationship with the GDPR on this point, and possibly explicitly allow for such lists to be developed under very stringent conditions. The Dutch government has concluded that this type of lists could be an important means to improve the gatekeeper function.

Equally useful in this regard would be for the public sector to share lists of high risk individuals with obliged entities (e.g. listings of "most-wanted" individuals, be-on-the-lookout notices, arrest warrants, etc) which would act as a highly effective safety net.

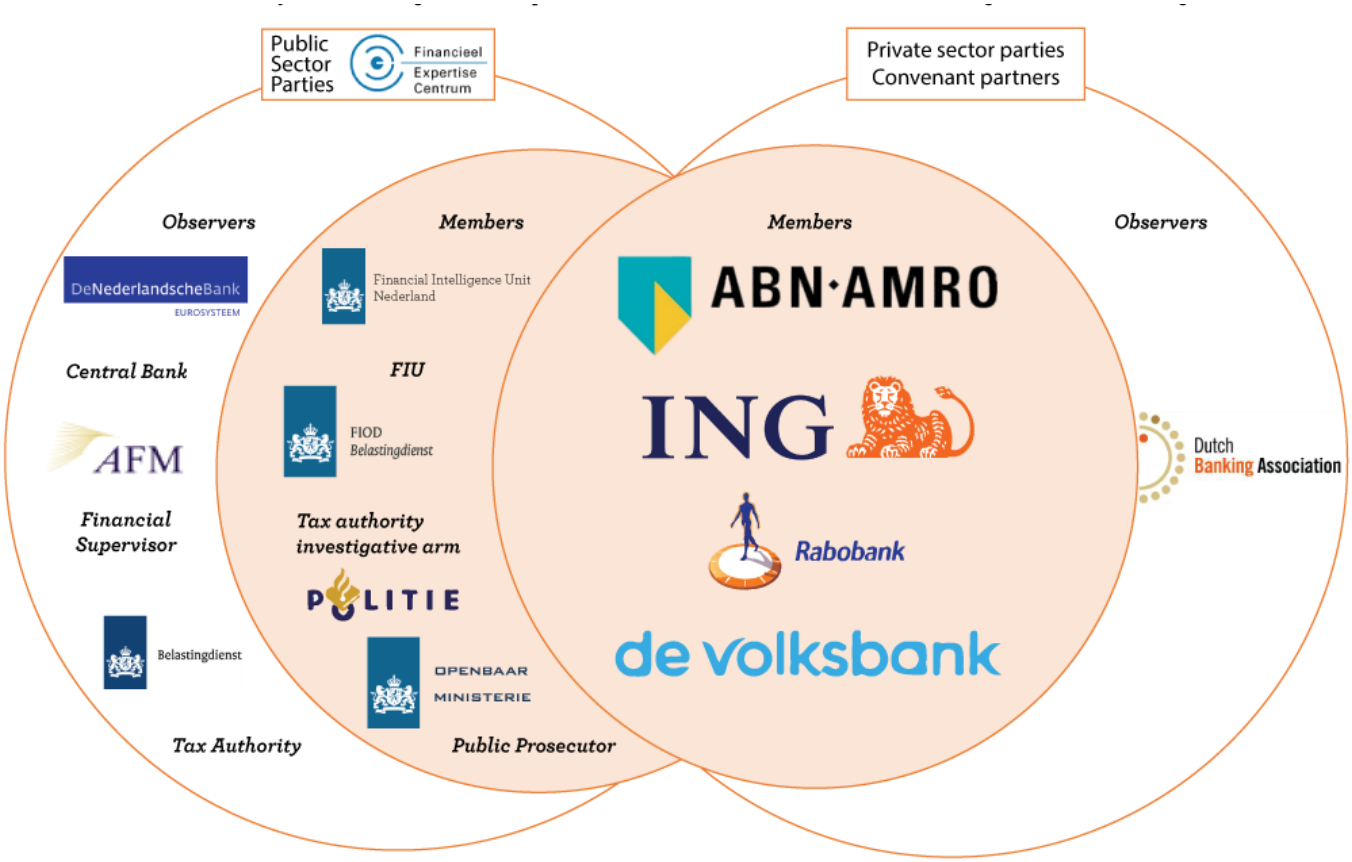
Access to UBO data – As explained in point 3.1. about harmonising EU legislation, we believe there should be an EU wide provision granting gatekeepers will full access to reliable UBO registers and allow gatekeepers to use that information for their due diligence requirements as well as to provide UBO register with alerts regarding false information.

Better public-private feedback loops – For banks to be able to effectively contribute to fighting financial crimes, the feedback loops between the public and private sector (in both direction) are crucial. For example, feedback from FIUs when banks file a suspicious activity report would significantly improve the banks' ability to improve its own systems and processes

Policy recommendations:

- *EU policy makers should encourage public-private partnerships to fight financial crime, and clarify the conditions for operational data sharing between actors*
- *EU law should explicitly allow certain forms of cooperation between gatekeepers where cooperation will improve the gatekeepers' effectiveness. This includes shared KYC and transaction monitoring utilities, as well as the development of "red flag" high risk clients.*
- *On top of encouraging cooperation agreements, EU law should also encourage stronger feedback loops between public and private gatekeepers.*

Dutch Banking Association



Objective: work together on the prevention and the detection of serious crime through information sharing