Joined forces

Towards a more effective and efficient fulfillment of the gatekeeper role in the Netherlands

KPMG Advisory N.V.

Amstelveen, August 23, 2023

143 pages

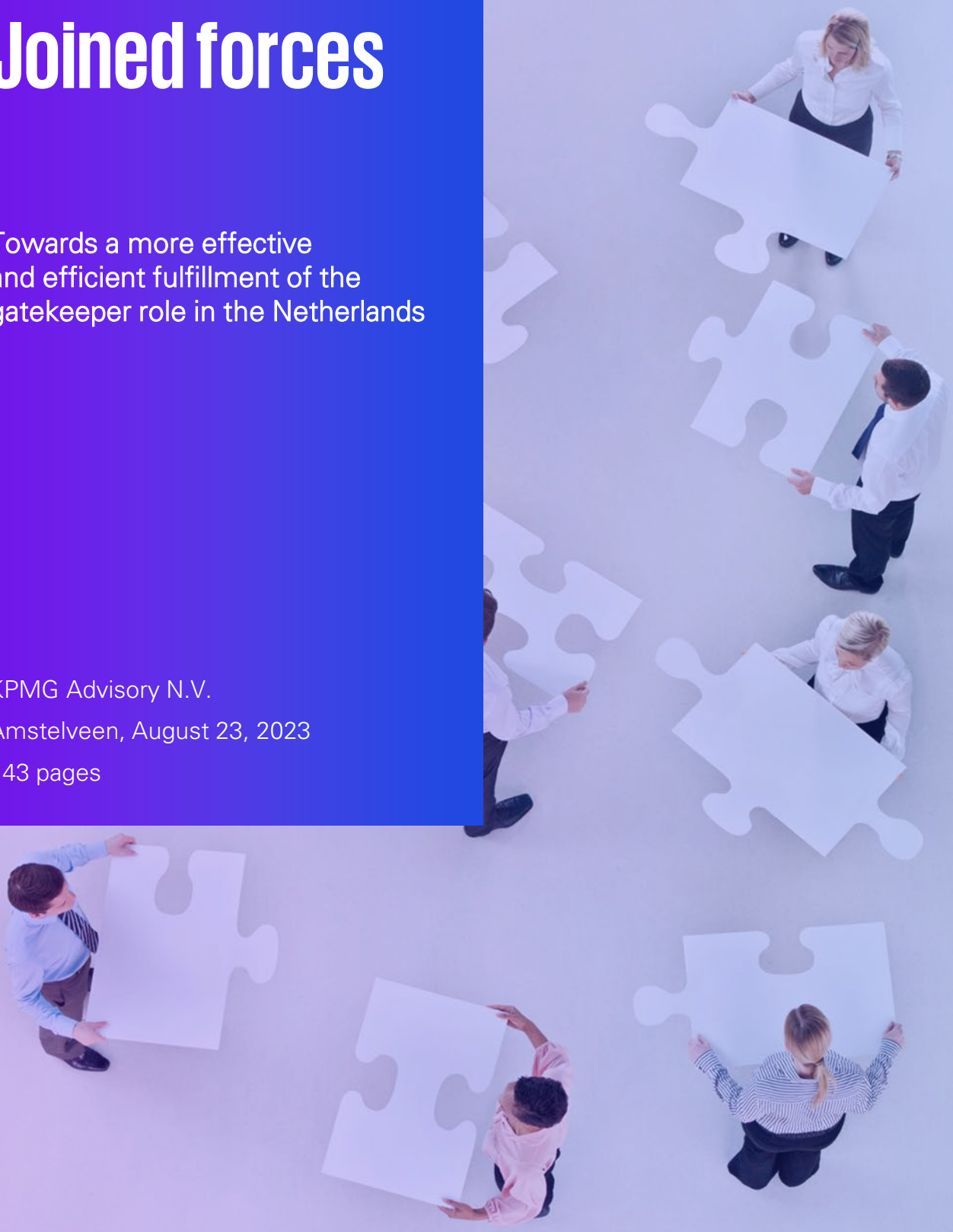


Table of contents (1)

Table of contents (2)

Management summary

Background

The Dutch financial system can be misused by criminals to launder illegally obtained assets or to finance terrorism. To prevent this, the Money Laundering and Terrorist Financing (Prevention) Act (Wwft) imposes measures on financial institutions and professional service providers – the so-called gatekeepers. Gatekeepers also have to deal with obligations arising from the Sanctions Act 1977 (Sw) and often with specific laws and regulations or professional standards as well. Some financial institutions, such as non-life insurers, do not fall under the Wwft, but are expected to comply with the Sw.

With this study the opportunities and possibilities of improving the efficiency and effectiveness of the anti-money laundering chain and compliance with the Sw through the collaboration of the various groups of gatekeepers or by applying creative other methods, were explored.

This study was conducted in the period from mid-March to the end of June 2023 by KPMG Advisory N.V. (KPMG) at the request of the Nederlandse Vereniging van Banken (NVB, the Dutch banking association), the Verbond van Verzekeraars (the Dutch association of insurers), the Nederlandse Coöperatieve Vereniging van Makelaars en Taxateurs in onroerende goederen NVM U.A. (NVM) and the Vereniging VBO – Vereniging van Makelaars & Taxateurs (VBO) (both associations of real estate agents and appraisers), the Koninklijke Notariële Beroepsorganisatie (KNB, the Dutch association of civil-law notaries), Holland Quaestor (the Dutch association of trust offices), Vereniging VNO-NCW (VNO-NCW, the largest employers' organisation in the Netherlands) and the Koninklijke Vereniging MKB-Nederland (MKB-Nederland, the largest entrepreneurs' organisation in the Netherlands).

Gatekeepers: a heterogeneous group

Although the objective and obligations under the Wwft are the same for all gatekeepers, they are a heterogeneous group and differences in emphasis can be discerned in gatekeepers' roles and responsibilities. Institutions and professionals have been brought within the scope of the Wwft for various reasons. For example, banks and trust offices are designated as gatekeepers because they provide access to the payment system and the Dutch economy, while, for example, for civil-law notaries this is the case because of the specific legal services they provide. Institutions and professionals may also be designated as gatekeepers because of the risk of misuse for money laundering purposes – such as real estate or cash – or because the nature of their services enables them to detect indications of fraud and other forms of financial and economic crime. Gatekeepers' relationships with their customers also differ. Some gatekeepers have long-lasting relationships with their customers. Other gatekeepers – such as real estate agents – on the other hand, have one-off or ad-hoc contact with customers.

Bottlenecks in the implementation of the Wwft and the Sw

In the performance of their gatekeeper role, gatekeepers encounter various bottlenecks in complying with the Wwft and the Sw. Some of these bottlenecks can be traced back to the fundamentals of the anti-money laundering policy. In the first place, there are tensions between the commercial interests of gatekeepers and the fulfillment of their gatekeeper role, sometimes complemented by societal expectations related to widely supported societal ambitions in areas such as sustainability, climate, environment, health, human rights and governance.

In addition, gatekeepers feel insufficiently supported by the government in various areas, due to, among other things, a lack of clear steering and prioritization by the government, conflicting laws and regulations, a lack of powers in light of the expanding Know Your Customer/Customer Due Diligence (KYC/CDD) obligations, uncertainty about the interpretation of the risk-based approach and the limited opportunity to learn due to the lack of an effective feedback loop. In particular, the tension between the protection of privacy on the one hand and the effective prevention of money laundering and terrorist financing on the other hand is experienced as a major limiting factor. This tension has recently manifested itself in several areas: access to the UBO register, the possibilities and impossibilities for information sharing between gatekeepers and public parties and between gatekeepers themselves, as well as in various legislative processes such as the Money Laundering Action Plan and Data Processing by Partnerships Acts. The experienced lack of support can frustrate gatekeepers and is detrimental to their motivation to guard the gate strictly.

At the same time, gatekeepers run the risk of facing serious penalties, in the opinion of that same government, they do not or do not sufficiently fulfill their gatekeeper role. This includes both administrative or disciplinary law enforcement by the regulators and criminal law enforcement by the Public Prosecution Service. This approach towards gatekeepers results in a situation where gatekeepers become tensed up and feel compelled to do more than necessary, which is also referred to as the ‘rule-based’ implementation of risk-based standards or as 'compliance-oriented’ adherence, just to make sure that they can demonstrate compliance with all requirements.

Customers increasingly experience this tension in the form of reduced access to the financial system. Natural persons and companies with higher integrity risks – for example, politically exposed persons (PEPs), associations, or foundations – may be faced with a refusal or restriction of services. Customers are also confronted with longer processing times at the start or with the expansion of services, as well as with higher costs and repeated (unnecessary) inquiries.

A deepdive into collaboration and other alternative working methods

Nevertheless, gatekeepers are increasingly aware of the importance of the gatekeeper role and want to organize this role more effectively and efficiently: for themselves and for their customers. Initiatives in the Netherlands and abroad show that the aforementioned bottlenecks can be (partly) solved by focusing on collaboration and the use of (new) technologies. Central government steering, which allows the government to speak (more) with one voice, to make clear choices and to set priorities, can also contribute to an increased effectiveness and efficiency.

Mutual collaboration gatekeepers

In terms of collaboration, the development of joint utilities by gatekeepers, as well as the commitment to public-private partnerships, are notable. Information sharing is seen as an important cornerstone for an effective anti-money laundering policy.

Worldwide experiments are being carried out with varying degrees of success with joint utilities in the field of transaction monitoring, sanctions screening and (aspects of) the CDD process. The various initiatives involved in this deepdive show that such joint utilities can help to shorten the CDD process and consequently lead to a decrease in costs. Available data is, so to speak, reused, updated and enriched, which means that repeated inquiries to customers are no longer necessary. With regard to transaction monitoring, it is pointed out that network analyses allows more to be seen than an individual gatekeeper could – as a result of which the identification of unusual and suspicious behavior can be more targeted. In addition, reference is made to the possible increased efficiency of the transaction monitoring process, cost reduction through the joint development and maintenance of utilities, and improved risk management.

This study demonstrates that setting up and operationalizing a joint utility is no easy task and requires careful consideration of various aspects. These aspects include, among other things, the technology, the participants and governance, the type of information and actualization, the type of customers, the functions of the facility (for example, data collection and/or validation of data), data standardization, privacy and other matters such as intellectual property, competition and cybersecurity. These aspects play an important role and also (partly) influence the degree of success of initiatives that are developed at home and abroad.

Collaboration between gatekeepers may also involve the use of warning systems to make gatekeepers' customer investigations more effective and to keep the financial system 'clean'. One example is the Incident Warning System for Financial Institutions. This system designed for banks and insurers shows that information exchange between various (defined) private parties with the aim of more effectively preventing and combating misuse of the financial system – in this case fraud and deception – is possible. From a privacy perspective, the information exchange must be proportionate and subsidiary and the design of the system must have sufficient safeguards.

Public-private partnership

In addition to the foregoing, public-private partnerships (PPP) are also an important means of making the prevention of money laundering, terrorist financing and compliance with sanctions regulations more effective. The idea is that financial and economic crime can be better prevented by working together and by sharing knowledge and intelligence. PPPs can potentially help gatekeepers to improve their internal processes such as transaction monitoring and to perform their KYC/CDD processes in a more targeted manner. Within the EU, PPPs are on the rise, although their structure, objectives, participants and the type of information exchanged differ. In the Netherlands, public-private partnerships take place both on a phenomenon basis – such as by sharing typologies and trends – and on an operational level with regard to transactions, reports and/or (legal) persons. Examples of PPP initiatives in the Netherlands are Fintell Alliance NL, the public-private partnerships within the Financial Expertise Center (FEC), the Anti-Money Laundering Centre (AMLC) and the PPP within the National Information and Expertise Centre (LIEC) and the Regional Information and Expertise Centres (RIECs). This study demonstrates that public-private partnerships at operational level mainly take place with banks.

From this study, it appears that creating an equal relationship between the public and private partners is important. Mutual trust, perceived safety, commitment, understanding and sufficient transparency form an important basis for an effective PPP. This also applies to a proportionate deployment of people and resources, a clear (non-complex) governance and a clear recording of objectives, parties, and mutual roles and responsibilities.

Digital identity

With regard to the use of technology, in the context of KYC/CDD reference is made to the development and use of the digital identity, also known as e-ID. This is a digital account that can be used to verify a person's identity. Digital identities are not a new phenomenon in themselves and have been used for some time, especially by governments. That is why many digital identities to date have been developed by and for governments themselves.

The identification and verification of customers' identities is an important part of customer due diligence, with digital identities and applications playing an increasingly important role. Establishing business relationships at a distance, also referred to as non-face-to-face or remote onboarding, is becoming increasingly common, and the use of sufficiently reliable means of identification instead of regular identification documents, such as passports or driver's licenses, is allowed. More and more innovative technologies are being developed to facilitate the remote onboarding of customers. This could include identifying and verifying the identity of customers via video calling, signing documents digitally or through the use of biometric technology.

The development of the European digital identity with a wallet for both natural persons and legal entities offers opportunities for gatekeepers to make customer due diligence and ongoing monitoring of the business relationship more efficient. This study shows that both private and public parties can play an important role in the development and use of digital identities. However, succeeding in this requires a supportive government that enables the development of digital identities, and the use thereof, within the framework of the Wwft and Sw, both technologically and legally.

Central steering

Having a strategy based on a national risk assessment is important for central management. A good strategy sets frameworks, provides direction and allows for priorities to be set. Although careful steps have been taken in this direction in the Netherlands with the Money Laundering Action Plan of 2019 and the Policy Agenda to tackle Money Laundering dating from 2022, this study highlights that there is a clear need among gatekeepers for a government that manages (more) centrally, speaks (more) with one voice, makes clear choices and that sets priorities. The Dutch national risk assessments (NRAs) for money laundering and terrorist financing can be enhanced with elements from NRAs from abroad.

Furthermore, the Dutch government can learn from the national strategies as developed in Canada, the United States (US) and – in particular – the United Kingdom (UK). The strategies of Canada and the US focus specifically on anti-money laundering regulation, while the UK strategy takes a holistic, integrated approach to economic crime with anti-money laundering as one of its priorities. The UK strategy is by far the most detailed and has the greatest involvement from the private sector. This strategy contains concrete actions aimed at results, as well as clear governance, planning and deadlines. Lastly, this study also shows that Italy is an interesting country for the Netherlands; it has highly coordinated management via a national committee in which a large and diverse group of government organizations is involved. This shows the importance of a joint task remit in order to be able to share information with each other.

Possible solutions to enhance effectiveness and efficiency

This study presents various ways for gatekeepers to achieve improvements in effectiveness and efficiency of compliance with the Wwft and Sw through collaboration. However, the deepdive also highlights that the role of the government is crucial in order to increase the effectiveness of the overall anti-money laundering policy. This mainly concerns supporting gatekeepers, for example by removing (legal) obstacles for gatekeepers and committing to more structural collaboration between gatekeepers and public parties, to enable gatekeepers to better fulfill their role. This is also expected to contribute to the motivation of gatekeepers. Furthermore, for the government this entails taking control, allowing it to manage centrally at a high level and to setting priorities. This helps establishing an (even) stronger foundation for a clear and supported policy that enables gatekeepers to combat misuse of the financial system by criminals by effectively and efficiently preventing money laundering and terrorist financing.

There are several (possible) solutions that can be realized in the shorter and longer term to make compliance with the Wwft and Sw more effective and efficient and that contribute to realizing a more effective and efficient anti-money laundering approach. These have been selected and further elaborated on. The complexity and impact of these (possible) solutions differ. The (possible) solutions are divided into three clusters:

1. Solutions for which gatekeepers are primarily responsible.
2. Solutions for which gatekeepers and government must join forces.
3. Solutions for which the government is in the lead.

The below figure presents the selection of possible solutions. These will be explained in more detail hereafter.

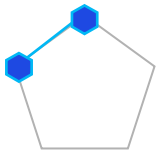
Gatekeepers	Gatekeepers and government	Government
• KYC taxonomy • Warning systems • Joint utilities	• Strengthening public-private partnerships • Use of digital identity (e-ID) in the context of customer due diligence	• Supportive government towards gatekeepers: – Reliable, public registers and adequate access for gatekeepers – Valuable feedback loop – Regulation of the real estate profession and a Wwft registration obligation for non-regulated professions and institutions – Protection gatekeepers in case of fear of retaliation – Public education about the role and responsibilities of gatekeepers • Taking ownership and providing for stronger central steering: – National coordinator – Strengthening, deepening and expanding the NRA – Setting priorities and establishing a risk appetite for the Netherlands

Table MS1: Overview of solutions

Gatekeepers

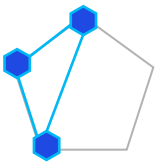
This study reveals a number of opportunities and possibilities for gatekeepers to take steps to improve the efficiency and effectiveness of the anti-money laundering chain and compliance with the Sw through collaboration. Basically, this requires mutual trust and knowledge exchange. Therefore, it is important that gatekeepers (continue to) commit to a (shared) understanding of each other's specific roles and responsibilities in the execution of the joint gatekeeper function, as well as to knowledge about the (nature of the) activities of various gatekeepers. It is also important to liaise on a structural basis to share developments, trends and phenomena. Moreover, gatekeepers should support each other with requests for help, given the nuances in roles, responsibilities and the diverse expertise of the various gatekeepers.

KYC taxonomy

Complexity	Impact
	

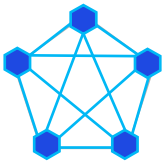
A first solution for gatekeepers concerns the development of a common standard in the field of KYC. The KYC taxonomy involves a joint interpretation of legal requirements, associated data points and underlying documentation. A shared KYC taxonomy ensures that gatekeepers collect the same information in a uniform, or harmonized, manner. This offers gatekeepers a stepping stone to the possibility of contributing to a more effective and efficient information sharing, because they have the same understanding of the information and thus speak 'the same language'. From a customer's perspective, a shared KYC taxonomy provides clarity and predictability and repeated (unnecessary) requests can be avoided.

Warning system

Complexity	Impact
	

A second solution for gatekeepers involves the creation of warning systems, if not already present, such as is the case for banks, insurers and trust offices. A warning system is a system that contains data from natural persons and/or legal entities that pose a possible risk to individual gatekeepers or to the integrity of the financial system, for example, in the event of serious suspicions or a conviction of fraud or other criminal behavior. This information is shared and used by gatekeepers (under certain strict conditions). Multiple parties know and see more than one: information sharing enables gatekeepers to identify risks better and faster, to limit these risks and to take adequate mitigating measures.

Joint utilities

Complexity	Impact
	

A third solution for gatekeepers concerns working towards joint utilities. In addition to the steps already taken by banks in the field of collective transaction monitoring – and where currently action on the side of the government is particularly desired with the further advancement of the Bill on the Money Laundering Action Plan – working towards a joint utility comprising various categories of gatekeepers with regard to (aspects of) the CDD process can make a positive contribution to efficient and effective compliance with the Wwft/Sw.

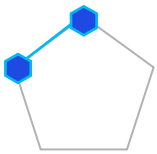
Initiatives from abroad show which aspects gatekeepers should thereby take into account. These aspects include, among other things, the group of participants, the type of customers, the desired functions of the utility, the type of information and actualization, the desired technology for the platform, the governance surrounding the utility and aspects such as privacy, competition and cybersecurity.

Based on the insights obtained during this study, it is advisable to start a joint utility (or several joint utilities) on a small scale. This can be done by limiting the circle of participants and the functions of the utility, for example, by limiting it to the collection of data and/or the validation of this data. It is advisable to keep the joint utility legally as simple as possible and to set it up for national use initially.

Gatekeepers and government

This study also presents a number of other opportunities and possibilities for improving the efficiency and effectiveness of the anti-money laundering chain and compliance with the Sw, whereby gatekeepers and public parties – respecting their own roles and responsibilities – must join forces.

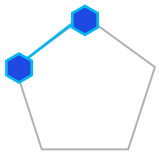
Public-private partnership

Complexity	Impact
	

In the first place, this concerns the continuation and expansion of a structural collaboration between public and private parties. Given the largely positive experiences of the operational collaboration between public partners and banks, it is recommended to consolidate this PPP and to expand it to other categories of gatekeepers. Gatekeepers and the government should take joint steps in this regard. In doing so, it would be necessary to ensure that not too many different forms of PPPs are created. It should also be prevented that concrete actions become subordinate to consultation and decision-making.

Furthermore, it is recommended that this new PPP be initiated via short and concrete pilots and to evaluate these pilots, in order to subsequently build towards a sustainable form of collaboration. It could also be considered to have categories of gatekeepers other than banks join existing PPP initiatives, such as the Serious Crime Task Force (SCTF) within the FEC. Creating an equal relationship between public and private partners is an important point of attention, as is a proportionate deployment of people and resources and a transparent (non-complex) governance and clear recording thereof. In order to really work together effectively and make an impact, it is essential that the government makes the (targeted) sharing of information - among public partners, among private partners, and between the public and private partners - legally possible.

Digital identity

Complexity	Impact
	

A second solution concerns (working towards) the use of digital identities in the context of customer due diligence. The use of digital identities and authentication tools offers various operational efficiencies in customer due diligence to both gatekeepers and customers. In anticipation of the digital passport, gatekeepers can already use digital authentication tools within the current legal frameworks of the Wwft/Sw. Gatekeepers can also use the development of the KYC taxonomy to determine for which data points and source documents it is desirable to link to the digital identities, and to share these wishes with the government. Lastly, gatekeepers can explore the possibilities for joining or developing a trust framework for the purpose of ensuring compliance with the Wwft/Sw. The government should promptly support the gatekeepers by clarifying which (providers of) identification tools meet the required 'substantial' or 'high' level of assurance.

For now, this is left to the individual gatekeepers themselves. This brings about uncertainty as well as a considerable effort for gatekeepers, and hinders (particularly small) gatekeepers from making use of such tools. It is also important that the government works on the rapid realization of the European digital passport and associated attributes, taking into account the desires of the gatekeepers.

Government

The time seems to have come for the government to motivate the gatekeepers more than before to fulfill their role to the best of their ability by offering them clarity and support 'at the front'. Going back to the core of the anti-money laundering policy, it is about the government taking a clear governing role, through which it provides (high-level) central steering and thereby prioritizes actions on the basis of the NRA.

A supporting government

Despite the fact that combating crime is a core task of the government, the government has assigned an important role to gatekeepers within its anti-money laundering policy. In order to optimally fulfill the gatekeeper role, it is important that gatekeepers are enabled to do so, for example, by offering them an adequate set of powers and the necessary clarity. To this end, five recommendations follow from this study:

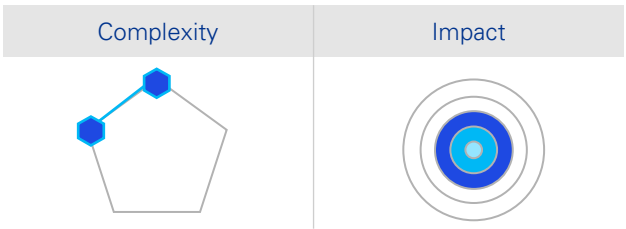
1 Work on reliable, public registers and ensure adequate access for gatekeepers

As a basis for relevant information and data for customer due diligence, data from public registers must be (as) reliable (as possible). To prevent extra work for gatekeepers, they should in principle be able to rely on this information. This includes the following concrete actions:

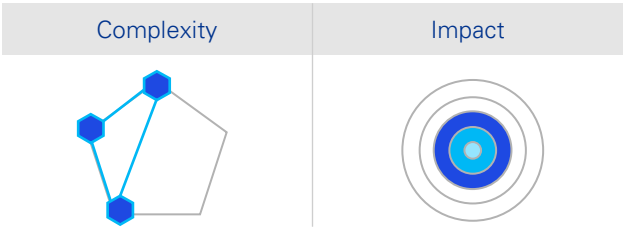
- Retain access to the UBO register for gatekeepers and all institutions that fall under the Regulation on Supervision pursuant to the Sanctions Act 1977 ("RtSw 1977") and grant them access to the closed section of the UBO register.

- Provide gatekeepers access to the Personal Records Database ("BRP") to perform their customer due diligence.

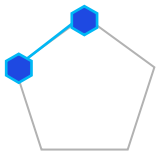
- Take action on ongoing legislative initiatives that can assist gatekeepers in complying with their Wwft obligations more effectively and efficiently, specifically with regard to the Central Shareholders Register ("CAHR") and enabling a 'search by name' of natural persons in the Business Register.



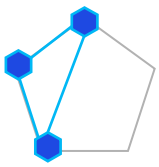
- Consider further support for gatekeepers by creating registers for which gatekeepers currently often have to use commercial providers, for example, with regard to creating a public PEP register and maintaining up-to-date sanction lists.



- Consider performing sanction checks against public registers by the government and relaxing the research effort of companies, for example, by assigning the Chamber of Commerce the task of performing sanction checks on the information included in the UBO register or Business Register.

Complexity	Impact
	

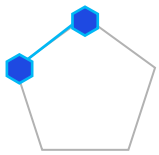
2 Create a valuable feedback loop

Complexity	Impact
	

The call for an effective feedback loop from gatekeepers may have existed as long as the reporting obligation itself. Aggregate feedback is already shared with gatekeepers. What is still missing is individual feedback at the level of the reporting organization or the transaction to which the report relates. Gatekeepers can learn from this and this can have a positive effect on their willingness to report and the quality of their reports.

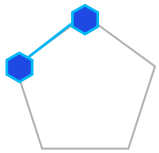
For the creation of a valuable feedback loop a start can be made by providing sector-wide feedback on outcomes of reports made by that sector over a certain period by the Financial Intelligence Unit-Netherlands ("FIU-NL"), possibly together with criminal investigation services, within the current legal frameworks. In addition, action should be taken in order to provide feedback on individual reports. With regard to transactions declared suspicious, it is valuable for gatekeepers to gain (more) insight into the use of the suspicious transactions reported by them in the criminal investigation process. Criminal investigation services and the Public Prosecution Service should therefore (be able to) provide feedback at least at an aggregate level, for example, in the form of statistics and by sharing case studies.

3 Regulate the real estate profession and consider introducing a Wwft registration obligation for non-regulated professions and institutions

Complexity	Impact
	

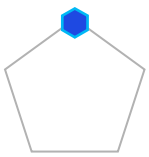
The real estate sector is vulnerable to money laundering and the unregulated real estate profession potentially makes the sector even more vulnerable: there are no minimum quality requirements, nor is compulsory membership of professional organizations required. It is therefore virtually impossible to find out how many real estate agents are actually active in the Netherlands, because not all brokers are affiliated with one of the three industry associations (NVM, VBO and VastgoedPro). This lack of definition may also have an impact on the allocation of powers. Given the importance of the gatekeeper role and the need for a good balance between tasks and competences, it is appropriate to reintroduce regulation of the real estate profession. It is important to include the lessons of the past in shaping the regulation of the profession. Regulation of the real estate profession can go hand in hand with the introduction of a Wwft registration obligation for non-regulated professions and institutions. Regulation of the real estate profession may also be accompanied by a reconsideration of the current Wwft requirements and practice with regard to client due diligence performed on counterparties by real estate agents.

4 Protect gatekeepers in case of fear of retaliation for reporting unusual transactions

Complexity	Impact
	

A bottleneck experienced by gatekeepers concerns the fear of retaliation when reporting unusual transactions to FIU-NL. A number of steps have been taken and various solutions are being explored to strengthen (the sense of) security of reporters, but more protection of gatekeepers is necessary. Where gatekeepers have a government-imposed duty to report, the government has a duty to protect the reporter.

5 Provide public education about the role and responsibilities of gatekeepers

Complexity	Impact
	

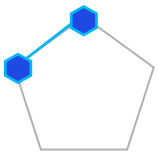
To enable gatekeepers to actually use their limited resources to fulfill their gatekeeper role, the government should provide more public education. Consideration could be given to maintaining a (digital) place where customers can find information about the roles and obligations of gatekeepers in complying with the Wwft and the Sw, launching a campaign, and setting up a questions and/or complaints office.

Central steering

The anti-money laundering policy in the Netherlands is characterized by a high degree of fragmentation. It is a standalone policy, but falls within the broader approach to organized crime. This means that many different government parties are involved, ranging from ministries, regulators, municipalities, FIU, government services and implementing organizations, criminal investigation services and the Public Prosecution Service. A lack of central steering, including clear prioritization and balancing of interests, can lead to the government not making clear choices, which leads to drifting and not going beyond general commitments. With an unambiguous government vision in which the various interests of government parties involved have been considered in advance and choices have been made, such 'paralysis' can be prevented and action can be taken. Clarity contributes to the motivation of gatekeepers, who can get to work in a(n) (even more) focused manner with the directions provided.

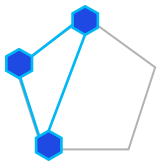
Specifically, this leads to three recommendations:

1 Appoint a national coordinator on behalf of the government who takes the lead in the national anti-money laundering approach

Complexity	Impact
	

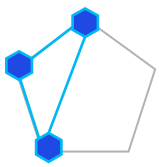
Ideally, the coordinator acts on the overall AML approach and connects the public parties and their interests involved. He acts as the driver of an effective and efficient anti-money laundering policy, and is the face or figurehead of this national approach on behalf of the government towards the private sector.

2 Strengthen, deepen and expand the national risk assessment

Complexity	Impact
	

National Risk Assessments ("NRAs") are the foundation for a national anti-money laundering strategy and the risk-based approach in the anti-money laundering policy. The Dutch government can learn from NRAs abroad. This concerns the methods of analysis used and the inclusion of sectoral and geographic risks in, or in addition to, the NRA.

3 Prioritize and establish a risk appetite for the Netherlands

Complexity	Impact
	

It is unrealistic to state that money laundering can be completely prevented with an effective application of the anti-money laundering policy. Nor is it realistic to expect gatekeepers to guard their gates in such a way that no criminal proceeds enter the financial system at all. With prioritization in a national anti-money laundering strategy, the activities of gatekeepers can focus on the most important national priorities. As not everything can be or remain a priority, this naturally also means that efforts will be less in other areas. It is therefore recommended that the Dutch government, together with the NRA and when setting its priorities, also establishes a national risk appetite that, together with the stated priorities, can serve as bandwidth for the application of the risk-based approach of the anti-money laundering policy, and thus for the gatekeepers in the fulfillment of their role.

From solutions to action

The extent to which the solutions will be realized and their full potential will be utilized will depend on the efforts and commitment of gatekeepers and the government. For gatekeepers it is essential that they (dare to) take the concrete steps within the possibilities available to them.

It is important for the government to enable the gatekeepers to do so. This concerns providing gatekeepers with powers as well was the removal of (legal) ambiguities or conflicts. In view of the expected impact, working towards strong central steering is of fundamental importance. Central steering requires a clear national anti-money laundering approach laid down in a strategy that is based on the actual risks for the Netherlands, and in which clear choices are made with regard to priorities in the fight against money laundering and terrorist financing.

Many solutions are affected by the current debate about privacy. The highest priority must therefore be given to balancing the importance of privacy on the one hand, and the prevention of money laundering and terrorist financing (and, by extension, the fight against crime) on the other.

In short, it is time to turn good intentions into concrete actions. This study shows that this can mainly be done by focusing on collaboration and the use of technology. Gatekeepers cannot do this alone. The government cannot do this alone. This can only be achieved together. Based on trust.

Introduction

1.1 Background and relevance

The Dutch financial system can be misused by criminals to launder illegally obtained assets or to finance terrorism. To prevent this, the Money Laundering and Terrorist Financing (Prevention) Act Wwft) imposes measures on financial institutions and professional service providers - the so-called gatekeepers. These gatekeepers are responsible for preventing their services from being misused by criminals. They do this by, among other things, carrying out customer due diligence (CDD), monitoring the business relationship and reporting unusual transactions. Pursuant to the Sanctions Act 1977 (*Sanctiewet*; Sw), natural persons and legal entities are prohibited from making money or other financial resources available to sanctioned persons or entities and, where applicable, from offering them certain financial or other services. Although the Sanctions Act has a wider scope of application, gatekeepers also have an important societal role in this regard. In addition, various gatekeepers are also subject to specific legislation and/or professional standards with additional obligations tailored to their services. This is, for example, the case for trust offices and civil-law notaries.

The various groups of gatekeepers have the same objective, but act at different points in time and also deal with differences in laws and regulations at times. In part because of this, gatekeepers encounter various bottlenecks that impede effective and efficient compliance with the Wwft and Sw. Some of these bottlenecks can be traced back to the fundamentals of the anti-money laundering policy. With society's increasing focus on privacy, there is currently a lot of discussion about the protection of privacy in relation to the (growing) obligations on gatekeepers related to the prevention of money laundering and terrorist financing.

The tension has recently manifested itself in several ways: regarding access to the UBO register, the possibility of information sharing between gatekeepers and public-sector parties and between gatekeepers themselves, as well as in various legislative processes such as the Money Laundering Action Plan and Data Processing by Partnerships Acts. Other bottlenecks could be solved through collaboration or by applying other creative working methods. This study explores such possibilities by taking a look 'across the sectors'. Although the study focuses on the situation in the Netherlands, the deepdive also includes relevant initiatives from abroad. The possible solutions that are presented are relevant to a broader group of gatekeepers and to the government.

This study was conducted by KPMG Advisory N.V. (KPMG) at the request of a group of eight industry and professional organizations in the period from mid-March to the end of June 2023.(1)

The groups of gatekeepers involved include banks, life and non-life insurers, real estate agents, civil-law notaries and trust offices. MKB-Nederland and VNO-NCW coordinated the study on behalf of the engaging parties.

1.2 Research questions

This study aims to explore the opportunities for and possibilities of improving the efficiency and effectiveness of the anti-money laundering chain and compliance with the Sanctions Act through the collaboration of the various groups of gatekeepers or by applying other creative working methods.

(1) The organizations are: Nederlandse Vereniging van Banken (NVB, the Dutch banking association), Verbond van Verzekeraars (the Dutch association of insurers), Nederlandse Coöperatieve Vereniging van Makelaars en Taxateurs in onroerende goederen NVM U.A. (NVM), Vereniging VBO - Vereniging van Makelaars & Taxateurs (VBO) (both associations of real estate agents and appraisers), Koninklijke Notariële Beroepsorganisatie (KNB, the Dutch association of civil-law notaries), Holland Quaestor (the Dutch association of trust offices), Vereniging VNO-NCW (VNO-NCW, the largest employers' organisation in the Netherlands) and Koninklijke Vereniging MKB-Nederland (MKB-Nederland, the largest entrepreneurs' organisation in the Netherlands). The study was completed on June 27, 2023.

The objective of the study is answered on the basis of the following sub-questions:

1. What are the roles and responsibilities of each individual gatekeeper?
2. Which bottlenecks do gatekeepers encounter when performing tasks whilst fulfilling those roles and responsibilities?
3. Can collaboration with other gatekeepers or an alternative working method eliminate those bottlenecks?
    - Do collaboration and the alternative working methods contribute to effective and efficient compliance with the Wwft obligations?
    - Do collaboration and the alternative working methods contribute to effective and efficient compliance with the Sanctions Act?
    - What hinders that/those form(s) of collaboration?
4. Are there international alternatives that lead to more efficient and/or effective working methods?
5. What steps can be taken to make improvements?

Reading guide

This report is structured as follows.

Chapter 2 provides insight into the roles and responsibilities of various gatekeepers.

Chapter 3 focuses on the implementation practice and bottlenecks encountered in that regard.

Chapter 4 contains relevant (international) examples in the area of collaboration and alternative working methods of gatekeepers that are, or could be, relevant to the Dutch practice and the matter of effective and efficient compliance with the Wwft and the Sw.

Chapter 5 describes possible solutions and specific steps that can be taken in that regard to achieve more effective and efficient compliance with the Wwft and the Sw through collaboration and alternative working methods.

1.3 Objective and limited distribution of the report

The distribution circle of this document is limited to our engaging parties for the purpose of, in the context of the engagement provided to KPMG, informing them of the work carried out to date, the insights derived from it, and the fine-tuning of these insights for the purpose of further developing the study.

It is not permitted to use this report or parts of it for other purposes, to cite or refer to it, to disclose it to the public and/or to provide it to third parties without our express and prior written consent.

1.4 Delineation of the study

For the purpose of this study, the concepts of effectiveness and efficiency, as well as the delineation of the study, are explained.

Effectiveness and efficiency

The research question makes a distinction between effectiveness and efficiency of compliance with the Wwft and Sw.

- Effective compliance is about the *purpose that the laws and regulations intend to achieve*. In other words, is the relevant legislation effective at preventing money laundering, terrorist financing and sanctions violations? This concerns effectiveness at the meta-level because it deals with the larger issue of whether the anti-money laundering system as we currently know it, based on the Wwft and Sw, actually contributes to - in a nutshell - less financial and economic crime.
    - Effective compliance also focuses on whether the *legal requirements are met* within this policy or system; in this study, these are the obligations stipulated in the Wwft and Sw that apply to gatekeepers.

- **Efficient** compliance is about the *efficiency of meeting current legal obligations*. This involves the question of whether there are ways to meet the legal requirements with fewer resources and less effort.

Focus on the Netherlands

The anti-money laundering policy and sanctions regulations are (as of yet) national laws and regulations.[2] Foreign initiatives are involved and analyzed in this study.

In light of the research question and sub-questions, the possible solutions are limited to the Netherlands.

1.5 Research method

This study was performed through a combination of different research methods.

A literature study provided the basis for the analysis of bottlenecks and opportunities, and possibilities for more effective and efficient compliance with the relevant legislation. The literature study led to an initial inventory of bottlenecks encountered by gatekeepers and customers, factors that could eliminate these bottlenecks, and some other possible solutions for achieving improvements in effectiveness and efficiency.

Qualitative, semi-structured interviews were held with representatives of the industry and professional organizations involved in this study, and with some Wwft regulators, the Financial Intelligence Unit-Netherlands (FIU-NL), the Public Prosecution Service, as well as some experts from academia and practice, to verify insights gained from the literature study and to gain additional insights. [3] Refer to Annex C for the whole list of interviewees.

Furthermore, through the international KPMG network and a network of experts from academia and practice, relevant domestic and foreign initiatives were identified that could serve as examples or inspiration for possible solutions in the Netherlands. This deepdive was conducted on the basis of the insights gained from the literature study and the interviews that were held.

(2) Refer to section 3.2.1 for European developments in the area of anti-money laundering regulations.

(3) Semi-structured interviews are interviews where a number of standard questions are determined in advance, and where there is leeway to expand on answers given during the interview or to ask additional questions.

Gatekeepers' roles and responsibilities

2

2.1 Introduction

This chapter examines gatekeepers' roles and responsibilities[4] in preventing money laundering and terrorist financing. Gatekeepers are private-sector parties designated by the government as important players in the prevention of money laundering and terrorist financing. The role of gatekeeper requires a large group of financial institutions and professional service providers - including banks, life and non-life insurers, trust offices, real estate agents and civil-law notaries - to know their customers and the risks they pose, and to mitigate those risks as much as possible. Where necessary, and as a last resort, they must refuse to provide or stop providing their services if they are not able to (adequately) mitigate the risks.[5]

Gatekeepers act in a broader ecosystem set up under anti-money laundering regulations. This is also called the 'reporting chain' or the 'anti-money laundering chain'. In this ecosystem gatekeepers deal with public-sector parties, like regulators, FIU-NL, the Public Prosecution Service and criminal investigation services like the police and the Fiscal Intelligence and Investigation Service (FIOD).[6] The following figure shows the division between private and public-sector parties in a simplified manner:

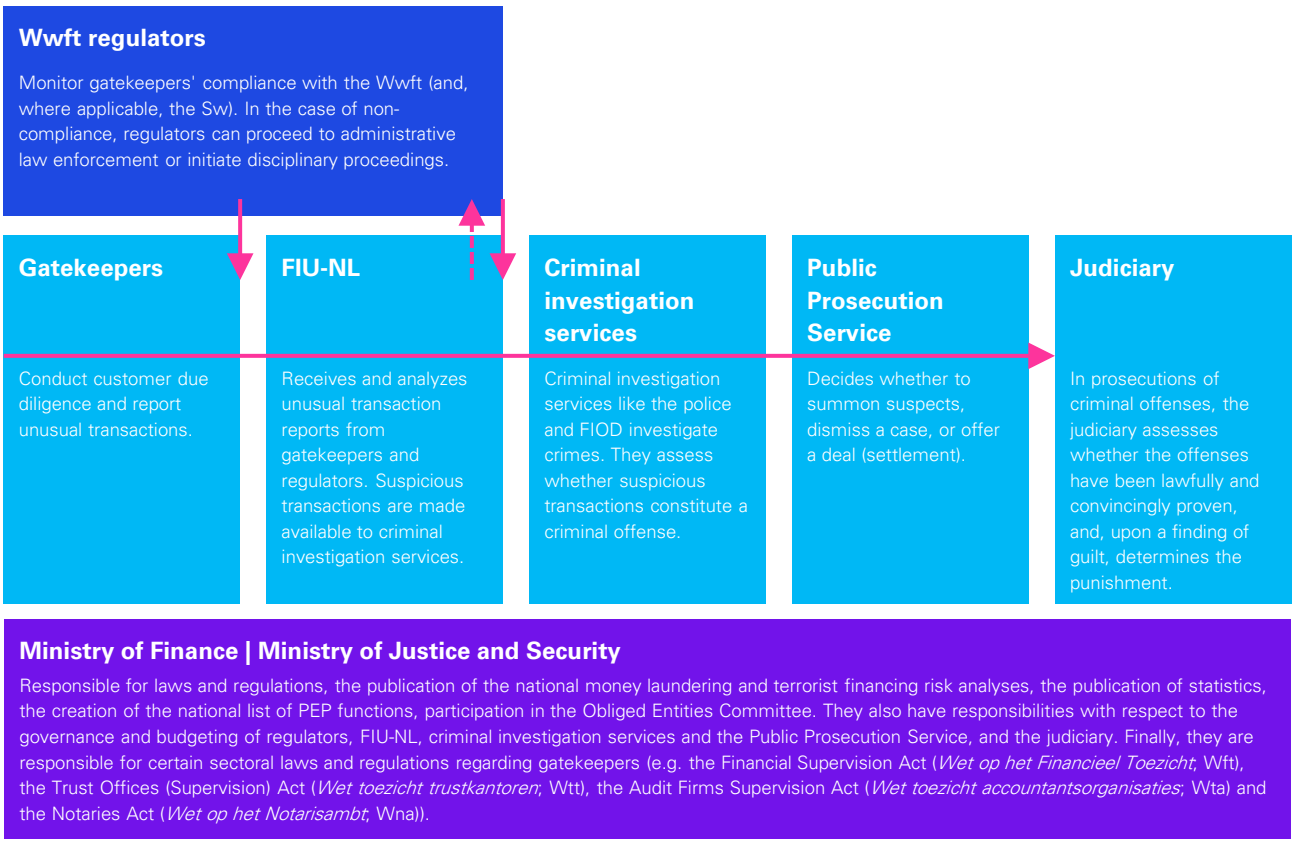


Figure 1: Division of the roles of public and private-sector parties within the anti-money laundering policy

(4) In this study, any reference to gatekeeper includes all institutions that fall within the scope of the Wwft. Non-life insurers also fall within the scope of this study even though they are only subject to the Sanctions regulations. The Sanctions Act applies to everyone in the Netherlands and, unlike the Wwft, does not have a gatekeeper function. Also refer to sections 2.2, 2.4 and 3.2.2. To avoid confusion, we have classified non-life insurers as 'gatekeepers' when referring to gatekeepers in the context of this study.

(5) Van Wingerde and Hofman 2022, p. 10.

(6) The terms 'government parties', 'public-sector parties', 'public-sector partners', and 'government' have the same meaning in this study.

In order to further clarify the roles and, in particular, the responsibilities gatekeepers have, the next sections describe the objectives ensuing from the Sanctions Act and the Wwft (sections 2.2 and 2.3). Section 2.4 discusses the specific roles and responsibilities of all gatekeepers.

2.2 Objective and obligations under the Sanctions Act

Sanctions are coercive measures that can be imposed on countries, companies, organizations or individuals when they pose a threat to international peace and/or security. The purpose of sanctions is to change undesirable behavior or make it more difficult, and thus to act as a deterrent to third parties. There are different types of sanctions including financial sanctions, trade restrictions, arms embargoes and travel and visa restrictions on certain individuals.(7) The different types of sanctions are not mutually exclusive.

The Sanctions Act (Sw) was drafted in 1977 and gives the Minister of Foreign Affairs the power to implement international sanctions (Section 2). The Sw covers international sanctions issued by, for example, the European Union and the United Nations.(8) Unlike the Wwft, the Sw applies to anyone situated in the Netherlands.(9) If financial sanctions are imposed, depending on the relevant sanctions regime, the assets of sanctioned persons or organizations are frozen. It is prohibited to make money or other financial resources available to them and, where applicable, to offer them certain financial or other services. The detailed obligations depend on the relevant sanctions regimes. Non-compliance with the Sw is an economic offence for which parties may be criminally prosecuted by the Public Prosecution Service.

Banks, pension funds, insurers, other financial institutions, regulated crypto service providers(10) and trust offices are subject to more specific sanctions obligations laid down in the Regulation on Supervision pursuant to the Sanctions Act 1977 (*Regeling toezicht Sanctiewet 1977*; RtSw 1977). A supervisory regime was also created exclusively for these institutions (Section 10 Sw). Under the Sanctions Act 1977 Legal Entities Designation Order (*Aanwijzing rechtspersonen Sanctiewet 1977*), the Dutch Authority for the Financial Markets (AFM) and De Nederlandsche Bank (DNB) were designated as the responsible regulators. If institutions do not comply with the specific requirements under the RtSw 1977, the regulators may impose administrative measures and sanctions on them.(11)

There are three core obligations in the Regulation on Supervision pursuant to the Sanctions Act 1977, which are briefly explained below:

1. Duty to have adequate controls

Institutions must adopt administrative organization and internal control (AO/IC) measures. This includes, at a minimum, adequate controls to assess whether the identity of a relationship corresponds to a sanctioned party, whereby assets can be frozen if necessary (Section 2). For AO/IC requirements, institutions can adhere to the requirements on organization and governance contained in the Financial Supervision Act (Wft), the Wtt 2018 or the Wwft. It should be noted that a relationship is defined in the Sw as 'any party involved in a financial service or transaction'. The concept of 'relationship' is thus broader than the concept of 'business relationship' in the Wwft.(12)

(7) Ministry of Finance, *Leidraad Financiële Sanctieregelgeving*, August 12, 2020, available via this link, p. 4.
(8) Ministry of Finance, *Leidraad Financiële Sanctieregelgeving*, August 12, 2020, available via this link, pp. 5-6.
(9) According to the *Leidraad Financiële Sanctieregelgeving* of the Ministry of Finance, p. 4, it applies to *'anyone situated in the Netherlands, to all Dutch legal entities and natural persons and all Dutch nationals outside the Netherlands'".*
(10) These are providers of custodian wallets for virtual currencies and providers offering services for the exchange between virtual and regular currencies.
(11) Section 10f Sw in conjunction with Sanctions Act 1977 Legal Entities Designation Order and Sections 10ba, 10c and 10d Sw.
(12) DNB, *Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act*, September 2022, available via this link, p. 71.

2. Reporting obligation

When an institution determines that a relationship has been sanctioned pursuant to the Sw (a 'hit'), it must report this (Section 3). Unlike unusual transactions reports under the Wwft, these reports should not be made to FIU-NL, but to the responsible regulator. This hit report must disclose the identity of the sanctioned party. However, one reporting obligation does not preclude another; a sanctions hit may also lead to the assumption of a possible unusual transaction within the meaning of the Wwft. In that case, institutions must report to both FIU-NL and the responsible regulator.(13) An institution may not generally terminate the relationship with the sanctioned party.(14)

3. Retention obligation

Section 4 requires institutions to retain records of reports and the relevant accounts and transactions for a period of five years after the sanctions regime no longer applies to the relationship in question.

The Sanctions Act imposes an obligation of result: institutions are required to comply with all sanctions regulations and thereby fulfill their obligations, including screening relationships.(15) In complying with sanctions regulations, a limited risk-based approach does appear to be permissible for business operations in terms of their AO/IC.(16) DNB indicates that all relationships should be screened, but that a risk-based interpretation may be applied to how the screening is carried out, for example, a lower frequency of screening or a less intrusive check.(17)

2.3 Objective and obligations under the Wwft

The Wwft entered into force in 2008 by combining the Provision of Services (Identification) Act (*Wet identificatie bij dienstverlening*; WID) and the Disclosure of Unusual Transactions (Financial Services) Act (*Wet melding ongebruikelijke transacties*; Wet MOT) and provides preventive measures in the policy against money laundering and terrorist financing.(18) The Wwft transposes several European anti-money laundering directives into Dutch law (see section 3.2.1 for more on this).

The objective of the law is to counter the laundering of illegally obtained assets and the financing of terrorism and - ultimately - to maintain the integrity and safeguard the stability and reputation of the financial system.(19) To achieve this objective, financial institutions and professional service providers have been assigned a gatekeeper function under the Wwft. The gatekeeper function means that these institutions and service providers have an important role in protecting, or providing access to, the legal and financial systems. In the case of accountants and civil-law notaries, for example, when the Wwft was introduced their gatekeeper role was indicated as giving legal force to transactions and thereby guarding "access to legitimate business," so to speak.(20) Based on the idea that combating money laundering through the private sector is more effective and efficient, increasing emphasis has been placed on the role and responsibility gatekeepers have in preventing money laundering and terrorist financing.

The Wwft system encompasses regulators monitoring gatekeepers' compliance with Wwft standards. In the event of non-compliance, administrative enforcement, and possibly disciplinary proceedings against certain professionals, may be initiated. Gatekeepers' non-compliance with the Wwft is also increasingly leading to criminal charges being brought against organizations and their directors.(21)

(13) DNB, *Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act*, September 2022, available via this link, p. 74.
(14) DNB, *Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act*, September 2022, available via this link, p. 70.
(15) Ministry of Finance, *Leidraad Financiële Sanctieregelgeving*, August 12, 2020, available via this link, p. 11.
(16) Bökkerink and Ligthart 2014, p. 214; Kodrzycki and Geertsma 2019, p. 234.
(17) Bökkerink and Ligthart 2014, p. 214; DNB, *Sanctions screening*, September 16, 2022, available via this link.
(18) Parliamentary Papers II, 2007/2008, 31 238, no. 3, p. 1.
(19) Parliamentary Papers II, 2007/2008, 31 238, no. 3, p. 1, Parliamentary Papers II, 2017/2018, 34 808, no. 3, p. 2.
(20) Parliamentary Papers II, 2007/2008, 31 237 and 31 238, no. 6, p. 3.
(21) Van Wingerde and Hofman 2022, p. 13.

In order to maintain the integrity of the financial system, the Wwft includes obligations with which gatekeepers have to comply.[22] In summary, these are currently the following five core obligations:

1. Risk management

Institutions need to be aware of which money laundering and terrorist financing risks they are exposed to and must tailor their policies, procedures and measures to these risks (Sections 2b and 2c). Institutions are required to take measures to identify and assess money laundering and terrorist financing risks, with the measures taken being proportionate to the nature and size of the institution.[23]

At a minimum, this takes account of risks related to clients, countries, products and services, and transactions and delivery channels. The risk assessment must be documented, kept up to date and be able to be shared with the regulator if requested.

The Wwft also has some obligations relating to gatekeeper governance, such as appointing a director to have final responsibility for the institution's compliance with the Wwft and having an independent and effective compliance function and audit function (Section 23).

2. Customer due diligence

Institutions are required to carry out risk-based customer due diligence before entering into a business relationship (Sections 3 and 4).[24] Customer due diligence includes the identification and verification of the customer's identity and, where applicable, of its legal representatives. Institutions need to determine whether a customer is acting on its own behalf or on behalf of a third party. Similarly, in the case of legal entities, institutions have to establish the identity of ultimate beneficial owners (UBOs) and take reasonable measures to verify that identity, as well as to understand the ownership and control structure of the legal entity.

The institution also has to establish the purpose and intended nature of the business relationship and conduct ongoing monitoring (Section 3). The Wwft also identifies a number of situations where simplified and enhanced customer due diligence are appropriate (Sections 6 to 9).

3. Reporting obligation

When institutions identify an executed or proposed unusual transaction, they must report it to FIU-NL without delay (Section 16).[25] The unusual nature of transactions must be determined on the basis of subjective and objective indicators.[26]

- If a transaction meets an *objective indicator*, institutions are always required to make a report to FIU-NL. An example for banks is a credit card or prepaid card payment amounting to EUR 15,000 or more.
- *Subjective indicators* involve situations where the institution has reason to believe that they could be linked to money laundering or terrorist financing, and this mostly depends on the circumstances of the case.

The reporting obligation also covers situations where the customer due diligence cannot be completed or a business relationship is terminated due to indications that the customer is involved in money laundering or terrorist financing.

Institutions may not unfairly discipline employees on the basis of a report made in good faith to FIU-NL, for example through demotion, a negative appraisal or exclusion.[27] As a general rule, institutions and their employees may not let anyone know that they have made a report to FIU-NL. This is also called the 'tipping-off ban'.[28]

(22) In line with the Wwft, trust offices are also subject to stricter obligations under the Trust Offices (Supervision) Act. This is further explained in section 3.2.3.
(23) For certain financial institutions listed in Sections 3:10, 3:17 Wft, and Section 10 of the Decree on Prudential Rules under the Wft (*Besluit prudentiële regels Wft*; Bpr), Section 19 of the Pension Funds Financial Assessment Framework Decree (*Besluit financieel toetsingskader pensioenfondsen*) and Section 14 of the Pension Act Implementation Decree (*Besluit uitvoering Pensioenwet*), the systematic risk analysis is broader and includes all integrity risks. The same applies to trust offices on the basis of Section 10 of the Decree on Trust Offices (Supervision) 2018. This is also known as 'SIRA' (Systematic Integrity Risk Analysis).
(24) There are some limited exceptions to this, see Section 4(3)-(6) Wwft.
(25) Transactions involve an act or a series of acts by or on behalf of a customer which the institution has become aware of in providing its services for that customer. So this can also cover partial payments or transactions that are connected.
(26) These indicators are listed in Annex 1 to the Wwft Implementation Decree 2018 (*Uitvoeringsbesluit Wwft 2018*).
(27) Section 20b Wwft.
(28) Section 23 Wwft. Only institutions operating within the same group may share this information within the group. See Section 23a Wwft.

4. Retention obligation

Under Section 33 of the Wwft, institutions are required to record relevant customer information in an accessible manner and to retain it for five years after the end of the business relationship or execution of the transaction.

5. Training obligation

Under Section 35 of the Wwft, institutions are required to ensure that employees undergo periodic training so that they are able to identify money laundering risks, to perform a proper and full customer due diligence screening, and to recognize unusual transactions. The board and, where applicable, the supervisory body must also undergo training to enable them to fulfill their responsibilities. Training must be kept up to date and thus regularly reviewed and revised. The content, depth and frequency of the training must be tailored to the positions of the relevant employees within the institution.(29)

Important changes to anti-money laundering regulations are imminent at both European and national levels. See section 3.2.1 for more on this.

2.4 Differences in gatekeepers' roles and responsibilities

Under the Wwft, various groups of financial and non-financial institutions, as well as professionals, have been designated as gatekeepers. They have been assigned this role because of their role as a professional service provider. As this role varies per institution and service provider, their exposure to money laundering and terrorist financing risks is different, and the sanctions requirements also differ between gatekeepers, differences in emphasis can be identified between different gatekeepers.

What follows is an explanation of the roles of the various (groups of) gatekeepers mentioned in the Wwft. The fact that some institutions also have to meet additional requirements under the Sw has already been explained in section 2.2.

Moreover, certain institutions and professionals are subject to additional sectoral legislation and/or (professional) rules that may reinforce or limit their compliance with their Wwft and Sw obligations.(30) This is discussed further in section 3.3.2.

The following section first discusses the groups of gatekeepers involved in this study, followed by the remaining gatekeepers.

2.4.1 Banks, insurers, trust offices, civil-law notaries and real estate agents

Banks

Banks play a key role in society in providing access to the payment system and are therefore an important party in ensuring the integrity and stability of the financial system. This key role - combined with the increased focus on combating money laundering and terrorist financing from the regulator, the Public Prosecution Service, society and the media - has led to the discussion on how to fulfill the gatekeeper role focusing on banks.(31) In the recent Financial Action Task Force (FATF) evaluation, the FATF concluded that within the group of non-financial institutions, a lot of institutions felt that customer due diligence is primarily a role for banks.(32) In recent years, banks have increasingly been confronted with their role as gatekeeper: regulator DNB has taken various enforcement measures for non-compliance with the Wwft, and banks and their directors have also been criminally prosecuted.(33) In addition to the Wwft, banks have wider integrity obligations under the Financial Supervision Act (Wft) and underlying regulations.

(29) DNB, *Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act*, September 2022, available via this link, p. 10.
(30) For example, banks, insurers and other financial institutions are subject to the Financial Supervision Act (Wft), trust offices are subject to the Trust Offices (Supervision) Act 2018 (Wtt 2018), civil-law notaries are subject to the Notaries Act (Wna), attorneys are subject to the Act on Advocates, and accountants are subject to the Audit Firms Supervision Act (Wta).
(31) Stichting Maatschappij en Veiligheid 2022, p. 14, and NVB 2022a, p. 13.
(32) FATF 2022b, p. 122.
(33) Stichting Maatschappij en Veiligheid 2022, p. 5.

One example concerns the extensive requirements around risk management and governance.

Insurers

The insurance industry comprises four different types of insurers: life insurers, non-life insurers, funeral expenses and benefits in kind insurers and reinsurers. Only life insurers have been designated as gatekeepers under the Wwft. The reason for this lies in the risk that the funds used to finance the insurance policies may be illegally obtained. In addition, there is a (limited) risk that policy benefits could be used to finance terrorism. It is because of these risks that financial service providers that mediate in life insurance policies have also been designated as gatekeepers under the Wwft.[34] The other types of insurers do not fall within the scope of the Wwft. These insurers do, however, need to comply with the additional obligations under the Sw.[35]

Like banks, insurers face wider integrity obligations under the Financial Supervision Act (Wft) and underlying regulations.

Trust offices

Given the nature of their services, trust offices play an important role in providing foreign legal entities with access to the Dutch economic environment. The literature argues that trust services can be misused to disguise ownership structures.[36] Customers may also pursue financial structures that pose certain tax integrity risks.[37] For these reasons, trust offices have a role to play in monitoring the integrity of the financial system and they have been designated as gatekeepers under both the Wwft and Wtt 2018. That last law contains additional, more detailed and stricter obligations around customer due diligence and also imposes some prohibitions on trust offices, as further elaborated in section 3.2.3. Recent attention has mainly focused on the risks of money laundering through illegal trust services.[38]

Civil-law notaries

Civil-law notaries are independent legal advisors who legally record agreements and statements that have been made in a notarial deed. They have been designated as gatekeepers due to their specific legal knowledge and role within the Dutch legal system.[39] Not all services provided by civil-law notaries fall within the scope of the Wwft: in a nutshell, the ones that do relate to corporate law and real estate.[40] These could include, for example, incorporating companies, purchasing or selling shares, or facilitating real estate transactions. A litigation exemption also applies: the Wwft does not apply to work surrounding the legal defense of clients.[41] The nature of the services provided by civil-law notaries combined with their duty of confidentiality under the Notaries Act (Wna) means that they are identified in the literature as an attractive professional group for criminals, which demonstrates the importance of their role as gatekeepers.[42]

Real estate agents and appraisers

The real estate industry is susceptible to money laundering and other forms of financial and economic crime. Real estate is a popular choice for investors because of its relatively stable - and generally rising - prices. Real estate is also functional: it can be occupied or rented out.[43] However, this also attracts criminals.

Factors that contribute to the susceptibility of the real estate industry to criminals include the limited duration of the relationship with customers, which makes it difficult for a real estate agent to identify suspicious circumstances or patterns, the potential for moving large cash flows when buying or selling real estate, a lack of transparency surrounding the valuation and pricing of real estate, and the possibility of high returns.[44]

(34) FATF 2018, p. 9.
(35) Section 10 Sw 1977 and Section 1 RtSw 1977.
(36) FATF 2019, p. 9.
(37) DNB 2019, p. 5.
(38) See section 3.2.3 for more on this.
(39) Van Wingerde & Hofman 2022, p. 10.
(40) Section 1a(4)(d) Wwft. See also: Snijder-Kuipers 2020, pp. 36-37.
(41) Section 1a(5) Wwft.
(42) On the duty of confidentiality, see Van Wingerde & Hofman 2022, p. 43.
(43) European Parliament 2019, p. 2.
(44) European Parliament 2019, pp. 1-2; FATF 2022a, pp. 16-17.

Given their services and expertise, real estate agents are expected to recognize indications of financial and economic crime. They have been designated as gatekeepers against this background. Unlike many other categories of gatekeepers, the real estate industry in the Netherlands is an unregulated profession and the title of real estate agent is not legally protected, which can make the industry even more vulnerable.(45) It has been pointed out in the literature that the lack of regulation may ensure that *"rogue real estate agents are more likely to enter the market and that they also cannot be expelled from the profession."*(46) Real estate agents have been designated as gatekeepers against this background. This applies both to the purchase and sale of real estate and to the brokerage and conclusion of leases where the monthly rent amounts to EUR 10,000 or more.(47)

Real estate appraisers determine the value of real estate and therefore also fall within the scope of the Wwft. This covers all types of appraisals related to real estate, for example in connection with a purchase or refinancing.

2.4.2 Other gatekeepers

Financial institutions other than banks or insurers

In addition to the aforementioned banks and insurers, there are several other financial institutions that have been designated as gatekeepers under the Wwft. These include (managers of) investment institutions and undertakings for collective investment in transferable securities (UCITS), investment firms, payment service providers and agents, electronic money institutions and exchange institutions. These institutions have been designated as gatekeepers due to the risk of their being misused to disguise the criminal origin of funds through large volumes of financial transactions (also known as 'layering').

Accountants, attorneys, tax advisors

Like civil-law notaries, accountants, attorneys and tax advisors have been designated as gatekeepers because of their specific legal, tax or financial expertise.(48) Criminals could misuse this expertise, for example to conceal ownership through complex legal ownership structures, or to disguise the criminal origin of funds.(49) Similarly, given the very nature of their services, accountants, attorneys and tax advisors may encounter suspicions of financial and economic crime. Think, for example, of indications of fraud found during audits of the financial statements by auditors.

Like civil-law notaries, not all services attorneys provide fall within the scope of the Wwft.(50) The litigation exemption described for civil-law notaries also applies to attorneys, tax advisors and professionals who carry out activities similar to those of attorneys or civil-law notaries.

Providers of crypto services

The virtual currency market has grown rapidly in popularity in recent years. Virtual currencies have certain characteristics that make money laundering attractive, including anonymity, the speed of transactions and the ease of cross-border transactions.(51) Given this perspective and with the advent of the Fifth European Anti-Money Laundering Directive and its transposition into the Wwft, custodian wallet providers and companies that offer services for exchanging virtual and fiduciary money have been designated as gatekeepers.(52)

(45) FATF 2022a, p. 16; Hoogenboom 2021, p. 171, notes that a significant proportion of real estate agents are not affiliated with trade associations and that the latter actually play an important role in creating and strengthening their gatekeeper function. He advocates reinstating the protected title of 'real estate agent' with mandatory membership of a, yet to be consolidated, trade association.
(46) Van Wingerde et al. 2023, p. 49.
(47) Section 1a(4)(h) Wwft.
(48) Van Wingerde & Hofman 2022, p. 10.
(49) FATF 2019a, pp. 12-16.
(50) Section 1a(4)(c) Wwft.
(51) FATF 2021b, p. 16.
(52) Directive (EU) 2018/843 of the European Parliament and of the Council of May 30, 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU, *OJEU* L-156, pp. 43-74.

With the imminent European Markets in Crypto Assets Regulation (MiCAR), the entire crypto sector will be subject to integrity requirements.[53] The current registration regime will be replaced by a tougher licensing regime, accompanied by more detailed standards in terms of their governance, which will cover more types of crypto service providers.

Gambling providers

With the introduction of the Remote Gambling Act (*Wet Kansspelen op afstand*) in 2021, online gambling providers have been included as gatekeepers under the Wwft in addition to Holland Casino. After all, online gambling is subject to many money laundering risks, including the possibility of anonymity, having a relationship at a distance ('non-face-to-face'), and complex and extensive transaction patterns.[54]

Luxury goods dealers, professional merchandise dealers and pawnbrokers

Dealers in luxury goods, both buyers and sellers, fall within the scope of the Wwft. Luxury goods include vehicles, yachts, works of art, antiques, precious stones, precious metals, jewelry and jewels. Dealers in works of art (art and cultural goods) have also been designated as gatekeepers, provided the payment for the work of art amounts to EUR 10,000 or more.

The value of art and cultural goods is difficult to estimate, which is why they are attractive for laundering money. Criminals may also choose to keep the art, art is frequently purchased with cash or through sham sales, and apparent legitimacy is given to funds that have been involved in fictitious sales and fake auctions.[55]

Professional traders, both buyers and sellers, fall within the scope of the Wwft to the extent that they facilitate cash payments of EUR 10,000 or more for goods other than the aforementioned luxury goods. It is common knowledge that cash is a suitable vehicle for money laundering because of the anonymity surrounding its origin, possession and use.

Domicile providers

Providers of (postal) addresses can potentially be misused by criminals. Merely providing a professional or business (postal) address (domicile provision) without additional work is not a trust service under the Wtt 2018. That is why these domicile providers have also been designated as gatekeepers under the Wwft.

2.5 Conclusions about gatekeepers' roles and responsibilities

It is clear from the foregoing that although the objective and obligations under the Wwft are the same for all gatekeepers, this is a large heterogeneous group and differences in emphasis can be identified in each party's role and responsibilities.

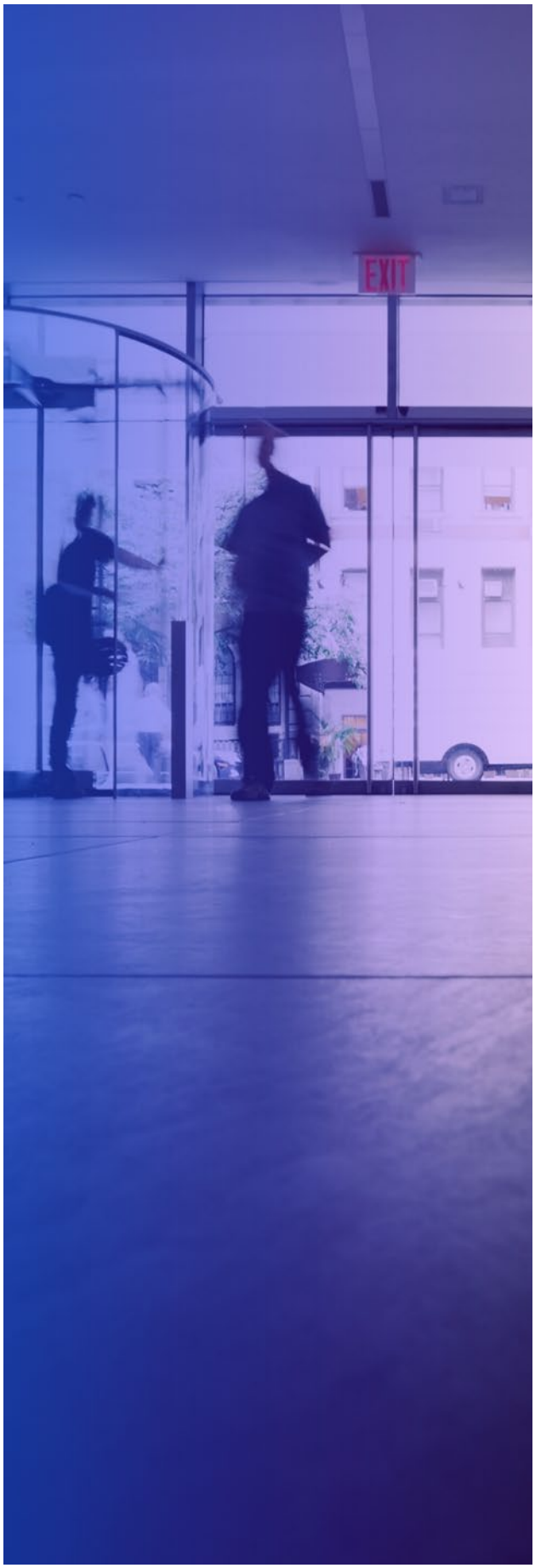
Institutions and professionals have been designated as gatekeepers for several reasons. Based on their services, they provide, for example, access to the payment system or the Dutch economy (banks and trust offices) or they provide specific legal, tax or financial services (for example, civil-law notaries, attorneys and tax advisors). Institutions and professionals may also have been designated as gatekeepers because of the risk of being misused for money laundering purposes - real estate or cash, for example - or because the nature of their services puts them in a position to spot indications of fraud and other forms of financial and economic crime. That is the case, for example, for accountants. In relation to the gatekeeper role, it is also notable that the duration of the relationship with customers is different for different gatekeepers. Sometimes they have long, enduring relationships with customers as is the case for banks, trust offices or auditors.

(53) DNB, "MiCAR important step in regulation of crypto markets", news report October 6, 2022. The regulation was adopted in May 2023: Council of the EU, "Digital finance: Council adopts new rules on markets in crypto-assets (MiCA)", press release May 16, 2023. It will enter into force on the 20th day after its publication in the Official Journal of the European Union and will be applicable 18 months later.
(54) European Commission 2022, p. 23; N. Boere, "Online gokken als witwasmethodiek", AMLC news report November 28, 2022.
(55) FATF 2023, pp. 21-22.

In contrast, other gatekeepers just have one-off or ad hoc contact with customers (for example, dealers in (luxury) goods, appraisers or real estate agents).

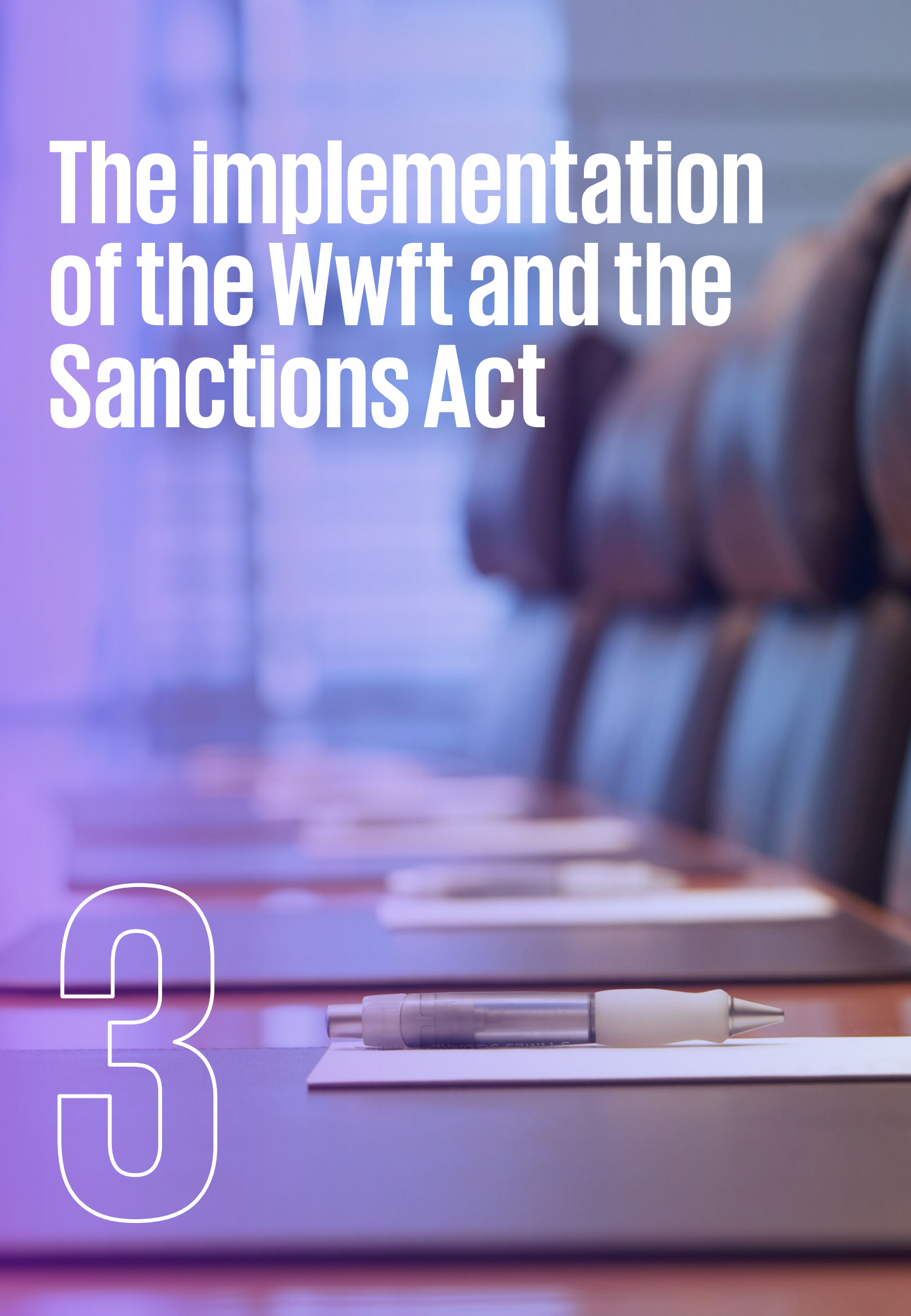
The Sw and its associated obligations apply to all gatekeepers. However, banks, insurers, other financial institutions, trust offices and crypto service providers have more detailed obligations compared to other gatekeepers and are regulated by the AFM and/or DNB. It is also worth mentioning that non-life insurers are not subject to the Wwft but are subject to the Sw and do not formally have a gatekeeper function.

Finally, it is noted that various gatekeepers also have to comply with sectoral legislation and/or (professional) regulations that may affect (the performance of) their gatekeeper role under the Wwft. This was already highlighted in this chapter with respect to banks, insurers, trust offices and civil-law notaries, among others, and will also be discussed further, where relevant, in Chapter 3.



The implementation of the Wwft and the Sanctions Act

3



3.1 Introduction

In order to explore opportunities and possibilities for improving the efficiency and effectiveness of the anti-money laundering chain and to ensure compliance with the Sanctions Act, it is important to know how things stand with respect to the implementation of the Wwft and the Sw. In this regard, it is useful to look at developments that have happened in recent years and expected developments in the short and medium term (section 3.2) as well as bottlenecks encountered or identified by the different stakeholder groups concerned (section 3.3).

3.2 Developments relevant to implementation

This section discusses developments to the Wwft and the Sanctions Act. It also discusses developments to the Trust Offices (Supervision) Act, because the Wtt 2018 partly extends the standards in the Wwft with standards that are stricter in nature. This section also focuses on relevant technological developments that have or could have an impact on the implementation of the Wwft and the Sw. Finally, given the tension found in the implementation of the Wwft and Sw, aimed at protecting the integrity of the financial sector on the one hand, and privacy regulations aimed at protecting the privacy of citizens and companies on the other, relevant developments in the field of privacy are also discussed.

3.2.1 Wwft developments in a nutshell

Chapter 2 already noted that the Wwft came into being in August 2008.[56] The Wwft is the result of transposing several European anti-money laundering directives, which in turn ensue from the FATF recommendations.

The FATF is an international organization which combats money laundering, terrorist financing and the financing of weapons of mass destruction.[57] The FATF publishes international anti-money laundering standards that form the basis for legislative and regulatory bodies worldwide when developing laws and regulations. In recent years, the Wwft has been amended several times as a result of changes to the FATF standards, and subsequently the European directives.

Anti-money laundering policy developments at European level are really taking off. Changes are succeeding each other at an increasingly rapid pace, which means that the Wwft is also subject to more frequent amendments. For example, whereas there were ten years between the Third (AMLD3[58]) and Fourth Anti-Money Laundering Directives (AMLD4[59]), there were just three years between the Fourth and Fifth European Anti-Money Laundering Directives (AMLD5[60]). On top of that, new European regulations have already been under discussion since 2019; and there has actually been work toward new European anti-money laundering regulations since July 2021 (see below).

With these successive regulations, the group of gatekeepers has also continually expanded. More and more private parties have come under the scope of anti-money laundering regulations in recent years, thus acting as gatekeepers. For instance, AMLD3 introduced trust and company service providers as a new group of gatekeepers. AMLD4 brought providers of gambling services and an extension to the group of persons trading in goods within its scope, and AMLD5 expanded the scope even further to include crypto service providers (custodian wallets and exchange services).

(56) Parliamentary Papers II, 2007/2008, 31 238, no. 3, p. 3.
(57) Bökkerink 2022, p. 196.
(58) Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *OJEU* L-309, pp. 15-36.
(59) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, *OJEU* L-141, pp. 73-117.
(60) Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, *OJEU* L-156, pp. 43-74.

Finally, substantive standards have also been extended enormously in recent years and gatekeepers are expected to do ever more in implementing the Wwft. New standards have been introduced, and existing obligations have become more detailed. These include an increased emphasis on the risk-based approach and sources that institutions have to take account of[61], the extension of enhanced due diligence measures in the case of domestic politically exposed persons (PEPs), the specific enhanced due diligence measures in the case of high-risk countries designated by the European Commission, the introduction of the register of ultimate beneficial owners (UBO register) and the duty to report discrepancies, plus requirements related to the governance of institutions like the compliance and internal audit functions.

Looking to the future

The aforementioned developments seem to be continuing at European level. Due to several money laundering scandals involving European banks as well as the publication of the Panama and Paradise Papers in which revelations relating to tax evasion and the avoidance of sanctions were made, in 2019 the European Commission took the first steps to achieving a stronger European regulatory framework.[62] In July 2021, it presented the so-called 'EU AML Package'.[63] This package consists of four legislative proposals:

- a new anti-money laundering directive ('AMLD6');
- an anti-money laundering regulation ('AMLR');
- a regulation establishing a new European Anti-Money Laundering Authority ('AMLA'); and
- a revision of the regulation on information accompanying transfers of funds.

The key things in the EU AML Package are the introduction of a uniform framework of standards for all institutions and professionals falling within the scope of the European anti-money laundering policy and the introduction of European regulation.[64] By transferring most of the substantive standard-setting to a European regulation that is directly applicable, the proposed Directive becomes more limited in comparison to AMLD5. AMLD6 will include standards for national registers, like the UBO register and the real estate register, as well as for the roles and responsibilities of national FIUs and regulators.

As of mid-2023, the AMLD6, AMLR and AMLA-R proposals were in the trilogue phase between the European Commission, the Council and the European Parliament. The revision of the regulation on information accompanying transfers of funds was subsumed by the aforementioned MiCAR and was finally adopted in May 2023.[65]

Important legislative changes are also expected at national level. In October 2022, after years of preparation, the Bill on the Money Laundering Action Plan was submitted to the House of Representatives.[66] This bill introduces amendments to the Wwft that relate to the joint monitoring of transactions by banks and the sharing of data between Wwft institutions of the same category on customers with a higher risk profile.[67] The bill follows on from a broader Action Plan from 2019 and aims to make the approach to money laundering in the Netherlands more effective.[68] More information on this bill and its relationship to privacy regulations is provided in section 3.2.5.

(61) For example, the EBA guidelines and the Supranational Risk Assessment (SNRA) published by the European Commission and the national risk assessments on money laundering and terrorist financing for the Netherlands.
(62) Groen and Van den Broek 2023, pp. 13-15.
(63) European Commission, 'Anti-money laundering and countering the financing of terrorism legislative package', press release July 20, 2021.
(64) Groen and Van den Broek 2023, p. 14.
(65) See section 2.4.2 on MiCAR. See also Council of the EU, 'Anti-money laundering: Council adopts rules which will make crypto-asset transfers traceable', press release May 16, 2023.
(66) The Money Laundering Action Plan dates from June 2019: Parliamentary Papers II, 2018/2019, 31 477, no. 41, Money Laundering Action Plan Annex.
(67) Bill on the Money Laundering Action Plan, Parliamentary Papers II, 2022/2023, 36 228, no. 2.
(68) Parliamentary Papers II, 2018/2019, 31 477, no. 41.

3.2.2 Sanctions Act developments in a nutshell

The Netherlands implements national and international sanctions measures based on the Sanctions Act 1977. UN sanctions were a commonly used tool in the 1990s, but the veto power given to permanent members of the UN Security Council means that, with geopolitical changes, it has become increasingly difficult for the UN to reach sanctions decisions.[69] Unilateral sanctions are now increasingly imposed by the European Union, as well as by countries like the United States and the United Kingdom.

The Russian invasion of Ukraine resulted in the sanctions landscape evolving at lightning speed; in just over a year, the EU adopted 11 sanctions packages.[70] Due to the difficulties in implementing and monitoring sanctions, partly due to the large number of public-sector parties involved, a National Coordinator for Sanctions Compliance and Enforcement was appointed in 2022. This National Coordinator was tasked with coordinating sanctions compliance between ministries and implementing organizations and identifying areas for improvement. The National Coordinator's report of findings was published in May 2022 and highlights various bottlenecks.[71] Examples include the structure of the Dutch economy, a fragmented supervisory landscape with restrictions on data sharing, and challenges in identifying UBOs. The report also notes that institutions that fall within the scope of the RtSw 1977 - including banks, insurers and trust offices - seem to prefer to apply sanctions rules too strictly rather than too loosely, suggesting 'overcompliance'.[72] Recommendations ensuing from this report focus, among other things, on intensified cooperation between all parties involved, the extension of regulation and the reporting obligation to the notarial profession, the legal profession and the accounting profession, and a stronger legal basis for exchanging data.

The Cabinet has announced that it is working on a full review of the Dutch sanctions system in response to the report's recommendations.[73]

Looking to the future

What the Dutch review of the sanctions system will look like is not yet known at the time of this study, nor is it clear how these changes will relate to developments at European level. In fact, with the aforementioned EU AML Package, shifts in European regulations will also take place: the evasion of targeted financial sanctions will explicitly be brought under the scope of the AMLR. Also, the latest available European proposals for AMLD6 provide for a full system of monitoring compliance with targeted financial sanctions by all relevant gatekeepers.

3.2.3 Wtt developments in a nutshell

The trust sector has been regulated since 2004: since that time trust offices have been subject to licensing and have to comply with the legal framework laid down in the Trust Offices (Supervision) Act. Revelations like the Panama Papers, investigations by regulator DNB and the results of the investigation by the Parliamentary Committee of Inquiry into Tax Structures prompted a large-scale review of the laws and regulations applicable to trust offices.[74] The Trust Offices (Supervision) Act 2018 (Wtt 2018) has formed the regulatory framework for trust offices since January 1, 2019. The main changes compared to the old Trust Offices (Supervision) Act concerned requirements around the professionalism and integrity of trust offices and customer due diligence.

(69) Van den Herik 2022, pp. 111-112.
(70) The 11th sanctions package was adopted in June 2023: Council of the EU, 'Russia's war of aggression against Ukraine: EU adopts 11th package of economic and individual sanctions', press release June 23, 2023.
(71) National Coordinator for Sanctions Compliance and Enforcement 2022.
(72) National Coordinator for Sanctions Compliance and Enforcement 2022, p. 13.
(73) Parliamentary Papers II, 2022/2023, 36 200 V, no. 56, pp. 5-9.
(74) Parliamentary Papers II, 2017/2018, 34 910, no. 3, p. 4; Riekerk 2016, p. 433.

For the trust sector, it is worth noting that the Wtt 2018 contains some specific and stricter requirements compared to the Wwft. Some examples include:

1. For trust offices, customer due diligence extends not only to the customer, but also (via Sections 27-30a Wtt 2018) to other parties involved in the provision of the trust service, like target companies, trusts or parties involved in the sale of a legal entity.(75)
2. The Wtt 2018 imposes an obligation of result on elements of the customer due diligence, specifically for situations where there are higher integrity risks. While this fits in with the risk-based system of the Wwft, it puts a heavier due diligence burden on trust offices.(76)
3. Trust offices have more limited options with respect to introductory customer due diligence when this has been carried out by another Wwft institution. Under the Wtt 2018, the due diligence has to be carried out by the trust office itself, or by a so-called 'introducing institution' within the trust office's group.(77)
4. Trust offices are obliged to investigate whether another trust office provides or has provided services to the customer or the target company, and whether a customer or the target company has been rejected in advance by another trust office.(78)

Although the Wtt 2018 is relatively recent legislation, it has already undergone several major amendments. The most recent amendments date from 2022 and the first half of 2023. A first important amendment concerns the ban on providing trust services to customers from certain countries. This ban was initially imposed on Russia and Belarus by means of an emergency measure following Russia's invasion of Ukraine in February 2022.(79)

This ban came into effect on July 16, 2022. By means of the Bill on the Integrity Measures for Trust Offices Act (*Wet integriteitsmaatregelen trustkantoren*; Wit), passed by the Dutch Senate on December 6, 2022, this ban will be extended to high-risk countries designated by the European Commission as having a higher risk of money laundering or terrorist financing or countries designated as non-cooperative on tax matters. A second amendment implemented via the Wtt was the ban on the professional or commercial use of conduit companies for the benefit of a customer. The background to this ban lies in tackling tax evasion and tax avoidance in the Netherlands. The Explanatory Memorandum states that "*making a conduit company available [...] serves primarily tax purposes and leads to a lack of transparency.*"(80)

Partly as a result of the increase in bans in trust legislation, the risk of illegal trust services has also been pointed out. Based on research, it has been estimated that "*in terms of the number of target companies [...] the market share of illegal trusts is therefore about 15 percent.*"(81) The problem with this is that these illegals are concealed from the regulator's view, which in fact means that there is even less of a grip on this group.(82) The problem of illegality has recently emerged from an investigation by the Financieele Dagblad (FD) and Company.Info into the impact of the emergency law banning trust offices from providing services to Russian customers.(83) The FD states that since the ban, Russian customers have been operating "*in the shadows*", this group is less visible and the fact that Russian customers are moving to parties other than regulated trust offices does not mean that "*money laundering and integrity risks are disappearing by themselves.*"(84)

(75) Parliamentary Papers II, 2017/2018, 34 910, no. 3, p. 4.
(76) Parliamentary Papers II, 2017/2018, 34 910, no. 3, p. 9.
(77) Section 23 Wtt 2018.
(78) See Section 68 Wtt 2018 in conjunction with Parliamentary Papers II, 2022/2023, 32 545, no. 180, p. 6. On the point of 'rejected in advance', Minister Kaag herself indicates that the law is not clear on this now and will be amended at the first suitable opportunity.
(79) Amendment to the Trust Offices (Supervision) Act 2018 in connection with an emergency measure to prohibit the provision of trust services to customers in the Russian Federation or the Republic of Belarus, *Bulletin of Acts and Decrees* 2022, 303.
(80) Parliamentary Papers II, 2021/2022, 36 102, no. 3, p. 2.
(81) SEO 2021, p. iv.
(82) See, for example, 'Nederland kent strengste trustwetgeving in EU', *Holland Quaestor* February 27, 2023.
(83) S. Motké, G. de Groot and J. Leupen, 'Hoe een 'zwart gat' in Amsterdam zich vult met Russen', *FD* March 24, 2023; G. de Groot, J. Leupen and S. Motké, 'Russische klanten gaan ondergronds na Nederlands trustverbod', *FD* March 24, 2023.
(84) FD Editorial Comment, 'Nederland heeft blinde vlek in trusttoezicht', *FD* March 28, 2023.

Looking to the future

Other developments are already afoot. On July 31, 2022, the report *De toekomst van de trustsector* (The future of the trust sector) was published.(85) It was commissioned by the Minister of Finance to examine whether trust service integrity can be adequately safeguarded. Researchers concluded that inherent integrity risks are primarily prompted by the "*international nature and complexity of transactions and ownership structures,*" and that the "*risks will not fully be eliminated as long as transactions passing through the Netherlands, ownership structures based in the Netherlands and the legitimacy of the origin of assets are not fully traceable*", but that these risks can be partly managed by the gatekeeper function of trust offices.(86) In response to the study, the Minister of Finance informed the House of Representatives of the follow-up steps, citing some relevant legislative proposals.(87) For instance, the consultation version of the Bill on the Financial Markets Amendment Act 2024 contains some tightening of the Wtt 2018: modification of the definition 'acting as a director', the elimination of the requirement for licensed trust offices to get prior permission from DNB for certain changes to the control structure, and a tightening up in relation to the implementation of tax advice by trust offices in connection with the ban on trust offices providing both tax advice and trust services to the same customer.(88) The Minister also indicated that she was considering some additional measures, including i) a clarification of the statutory provision on mandatory information sharing between trust offices in that it must also be verified whether customers have been rejected in advance by another trust office (to prevent so-called 'trust shopping'), and ii) increasing the transparency of trust offices (via a reporting requirement in the financial statements).(89)

3.2.4 Technological developments relevant to the implementation of the Wwft and the Sanctions Act

Technological developments also have an impact on the implementation of the Wwft and the Sw. These developments have the potential to contribute to more effective and efficient compliance with the legislation and thus combat financial and economic crime better.(90) Three developments are set out in what follows:

1. Digital identity and wallet

As outlined in Chapter 2, customer due diligence is a key obligation in the Wwft. An important part of customer due diligence is identifying the customer (and, where relevant, related parties like the UBO or legal representative) and verifying their identity. The move toward a digital identity for citizens and businesses could reduce the due diligence burden on gatekeepers because they will no longer have to request information from each individual customer, but will be able to access the digital identity if customers give them permission to do so.(91)

The Electronic Identification and Trust Services Regulation (eIDAS Regulation) was introduced in 2014 to enable electronic identification in Europe and to eliminate cross-border obstacles between national systems.(92) Among other things, the Regulation lays down agreements on the use of a mutual digital infrastructure and assurance levels. The eIDAS Regulation is currently under review. The European Commission has proposed that each Member State be required to develop an electronic identity (e-ID) and at least one digital wallet that can be used throughout the European Union.

(85) SEO 2022.
(86) SEO 2022, pp. 26-27.
(87) Parliamentary Papers II, 2022/2023, 32 545, no. 180.
(88) Consultatie voor de Wijzigingswet financiële markten 2024, April 29, 2022, available via this link.
(89) Parliamentary Papers II, 2022/2023, 32 545, no. 180, p. 6.
(90) DNB 2022, p. 28.
(91) DNB 2022, p. 28.
(92) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *OJEU* L-257, pp. 73-114.

In addition to identity data, the digital wallet could also contain other information like diplomas, address details and authorizations for representatives of legal entities.(93) Individuals would be able to identify themselves through the digital wallet and they could also choose which data they wanted to share through the wallet. Thus, an e-ID could contain more information than just identity data. The information shared could be tailored to the information the receiving institution needs.

Section 4.3 and Annex B further discuss developments and initiatives on digital identities within the European Union and beyond.

2. Artificial intelligence

Artificial intelligence ('AI') is an umbrella term for various technologies whereby machines can deploy skills like reasoning, planning and learning (for instance, Machine Learning).

While some of these technologies are good at finding deviations from a group, others can be used to learn from choices a person previously made and, in future, similar situations, evaluate what choice a person would have made. The potential benefit of AI is that the system can detect a deviation from a group - without actually having the knowledge of how individuals would come to this - and can thus detect new risks. At the same time, this potential benefit also carries a potential risk if AI is not properly implemented or is based on poor-quality data, leading, for example, to (undesirable) profiling and discrimination by the system.(94)

Although a survey carried out by KPMG in 2023 shows that most people are wary of trusting AI and it has a relatively low level of acceptance, its potential in preventing financial and economic crime is acknowledged.(95) It could make measures faster, cheaper and more effective.(96)

AI is already being used to some extent in the private sector for anti-money laundering purposes, for example in areas like customer risk analysis or transaction monitoring.(97)

The FATF refers, among other things, to the possibility of identifying risks better.(98) The EBA refers to speeding up customer due diligence, as well as document processing.(99) The Wolfsberg Group acknowledges that, with support from AI, institutions will be able to assess and monitor the risks inherent in customers and transactions in a more holistic way.(100) In the report 'From recovery to balance', DNB states that AI has the potential to contribute to more effective and efficient transaction monitoring. DNB does indicate in this regard that the quality of the data has to be high and that adequate safeguards must be put in place, in part to prevent unconscious discrimination.(101) In addition to its use for transaction monitoring, KPMG also points to the potential AI has in the area of sanctions screening.(102)

3. Blockchain technology

Blockchain is known as the technology behind crypto currencies, but it also has broader applications. Blockchain technology is a technology that can be used to make processes transparent and automate them. More and more companies are using blockchain technology to handle financial transactions and to support certain key processes, for example. Cryptography is used to store information in encrypted form. What makes blockchain technology special is that information is stored decentrally. This means that data can be stored without the intervention of a central authority or an independent third party and without being checked. The system is therefore not dependent on one central database.

(93) DNB 2022, pp. 29-30.
(94) European Parliament, *Artificiële intelligentie: Kansen en gevaren*, available via this link.
(95) KPMG 2023.
(96) FATF 2021, p. 4.
(97) See Institute of International Finance 2018; FATF 2021.
(98) FATF 2021, p. 24.
(99) EBA 2020, p. 20.
(100) Wolfsberg Group 2022a.
(101) DNB 2022.
(102) KPMG 2021.

In the context of combating money laundering and terrorist financing, blockchain technology could be a potentially suitable means for the (decentralized) exchange of information or for verifying the identity of citizens and businesses. The advantage of the technology is that the management of information remains with the 'owner' of the information.(103) Disadvantages of blockchain technology include its complexity and the need for specialized knowledge. Also, due to the absence of a central authority, all parties must want to cooperate.

3.2.5 Developments to privacy regulations and the impact these have on the implementation of the Wwft and the Sanctions Act

The General Data Protection Regulation (GDPR) has been in force in the European Union since May 25, 2018.(104) The GDPR has strengthened and expanded data subjects' privacy rights. The regulation places more emphasis than before on organizations' and companies' responsibility to demonstrate their compliance with the GDPR and has introduced a stricter supervisory and enforcement regime. With the introduction of the GDPR and increased media attention on privacy incidents and data breaches at public and private-sector parties - like the Dutch Childcare Benefit Scandal or the TikTok fine - privacy and the ethical handling of personal data are high on the social agenda.(105) Privacy awareness has also increased significantly.(106) One possible explanation for this lies in the further developments in the digital transformation that society is undergoing, within which the question of how responsible and/or ethical all technical developments are, is becoming ever more prominent.(107)

Despite the increased focus on the subject, the confidence that Dutch people have in how companies and public-sector parties deal with privacy continues to decline. In addition, more than half of Dutch people are concerned about the emergence of artificial intelligence (like algorithms) in relation to their privacy.(108)

In recent years, the Dutch privacy regulator, the Data Protection Authority (Dutch DPA), has also gained an increasingly prominent role. For example, the Dutch DPA has issued several heavy fines in the past two years.(109)

It is also notable that the regulator is getting involved more often in the public debate on government initiatives relating to personal data processing.(110) This results in public discussions in some cases, as is clearly the case with the proposed Bill on the Money Laundering Action Plan.

The tension between privacy legislation, the Wwft and the Sanctions Act

Given the increasing importance of, and focus on, privacy, it is increasingly noticeable that the protection of privacy clashes with other interests the government has to protect. The clash between the protection of privacy and other interests often manifests itself in the principles of proportionality and subsidiarity. A proportionality and subsidiarity assessment considers whether privacy infringements are reasonably proportionate to the objective to be pursued, for example, combating money laundering, and whether there are alternatives to achieve the same objective by means that infringe data subjects' privacy less.(111)

(103) This is discussed further in Chapter 4.
(104) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *OJEU* L-119, pp. 1-88.
(105) Dutch Data Protection Authority, *Boete Belastingdienst voor discriminerende en onrechtmatige werkwijze*, December 7, 2021, available via this link; Dutch Data Protection Authority, *Boete TikTok vanwege schenden privacy kinderen*, July 21, 2021, available via this link.
(106) KPMG 2023a, p. 1.
(107) In this regard, in the context of anti-money laundering policy, reference can be made to DNB, *Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act*, September 2022, available via this link, pp. 57-58, which provides that when transaction monitoring systems use forms of artificial intelligence, the institution can have a model validation or audit done to assess whether the system is working to a high quality and effectively. See also DNB's General principles for the use of Artificial Intelligence in the financial sector, which mention soundness, accountability, fairness, ethics, skills and transparency: DNB 2019a.
(108) KPMG 2023a, p. 2.
(109) See the overview of fines and other penalties on the Dutch Data Protection Authority's website, available via this link.
(110) Under Article 36(4) GDPR, it is mandatory for governments to seek the Dutch DPA's advice when drafting new laws and regulations relating to personal data processing.
(111) Article 5 GDPR lays down the principles relating to personal data processing; in this regard proportionality and subsidiarity play an important role in the context of data minimization.

The tension between the Wwft and privacy regulations has recently received due attention.[112] For instance, in November 2022, the European Court of Justice issued an important ruling on access to public registers containing information on ultimate beneficial owners (UBOs).[113] The Court ruled in two cases that the privacy of individuals is disproportionately infringed by giving the general public access to UBO registers, and declared that the European standard on which this is based is invalid.[114] As a result of this ruling, the UBO register in the Netherlands is unavailable for consultation for the time being, except to competent authorities like the criminal investigation services. The consultation on the draft Bill on Restriction of Access to UBO Registers (Amendment) Act provides for partial access to the UBO register to gatekeepers and institutions that exclusively fall within the scope of the RtSw 1977 (including non-life insurers).[115]

This is not the first time that privacy has been an issue in the context of the UBO register. In 2019, the Dutch DPA argued that the need for Wwft institutions to access the 'closed' part of the UBO register was insufficiently substantiated, and that for other financial institutions that fall under the Sanctions Act the description of the nature and scope of the problem was insufficiently clear.[116] Previously, the Dutch DPA had been critical of three designated special criminal investigation services having access to the closed part of the UBO register because, according to the Dutch DPA, the role these authorities had in combating money laundering was insufficiently substantiated.[117]

At European level, privacy regulators are also raising objections when it comes to the prevention of money laundering and terrorist financing. In the context of the aforementioned EU AML Package, privacy regulators, united in the European Data Protection Supervisor (EDPS), have already published several opinions and letters.[118] In the most recent letter, the EDPS expressed its opposition to the negotiating mandate of the Council of the European Union that pertains to allowing the sharing of personal data between private-sector and public-sector parties in the context of public-private partnerships, as well as the sharing of personal data between gatekeepers. The EDPS states that it has serious concerns about the legality, necessity and proportionality of these powers, arguing that these are insufficiently justified and do not have the appropriate safeguards. The EDPS therefore recommends that these provisions are not included in the final text of the AMLR.[119]

The impact of privacy legislation on the Bill on the Money Laundering Action Plan

The privacy discussion is also clearly present in the context of the Bill on the Money Laundering Action Plan, which attempts to make the Wwft more effective.[120] As indicated in section 3.2.1, this bill introduces amendments to the Wwft that relate to the joint monitoring of transactions by banks.[121] The bill provides for the joint monitoring of all business transactions and all transactions between individuals with a threshold of EUR 100. The rationale behind this is that banks currently have to monitor transactions individually and determine whether they are unusual. Banks do not get to see the entire transaction chain and unusual transaction patterns can therefore go undetected.[122] This bill also includes an obligation on gatekeepers belonging to 'the same category' to share information on services to customers with a higher risk profile that have been rejected, provided or terminated, to prevent 'shopping'.

(112) For example, RUSI 2016; EBA 2020; FATF 2021; FATF 2021a; Lagerwaard 2022; FATF 2022; Ipenburg 2023; Nuijten 2023.
(113) Court of Justice of the EU, November 22, 2022, C-37/20 and C-601/20, ECLI:EU:C:2022:912 (*WM v Luxembourg Business Registers* and *Sovim v Luxembourg Business Registers*).
(114) Ministry of Foreign Affairs | Expertisecentrum Europees recht, 'EU-regeling voor onbeperkte toegang van het publiek tot informatie over de uiteindelijk begunstigden van vennootschappen is ongeldig', news release December 2, 2022.
(115) See the proposed Section 22a(1) of the Business Register Act 2007 (*Handelsregisterwet 2007*) in the consultation of the Restriction of Access to UBO Registers (Amendment) Act. For a further explanation, see also pp. 14-19 of the accompanying draft Explanatory Memorandum. The consultation on the Restriction of Access to UBO Registers (Amendment) Act was launched on May 30, 2023 and is available via this link.
(116) Dutch Data Protection Authority 2019b.
(117) Dutch Data Protection Authority 2019a.
(118) EDPS 2020; EDPS 2021; EDPS 2023.
(119) EDPS 2023.
(120) Ipenburg 2023; Dutch Data Protection Authority, 'Nieuwe wet opent deur naar ongekende massasurveillance door banken', press release October 21, 2022; Dutch Data Protection Authority 2023; C. de Horde, R. Betlem, 'Felle verdeeldheid onder voor- en tegenstanders van nieuwe witwaswet', *FD* January 26, 2023; Nuijten 2023, pp. 146-147.
(121) Transactie Monitoring Nederland B.V. (TMNL) was established for the joint monitoring of transactions by banks. See section 4.2.1 and Annex B.
(122) Parliamentary Papers II, 2022/2023, 36 228, no. 3, pp. 9-10.

The Dutch Data Protection Authority has strong objections to the bill. According to the Dutch DPA, the proposal for the joint monitoring of transactions opens a door "*to unprecedented mass surveillance by banks*", which, in the Dutch DPA's view, amounts to a "*banking dragnet*".[123] The Dutch DPA has expressed concerns about the extent to which individuals' privacy could be infringed and believes that the bill is not necessary and violates the principle of proportionality. In the position paper prepared by the Dutch DPA as input for the roundtable discussion with the House of Representatives' Standing Committee on Finance, the Dutch DPA argues that surveillance could lead to individuals being excluded from the payment system and that there is a risk of unwarranted discrimination through the processing of special personal data like race, ethnicity and religion.[124] The bill is currently before the House of Representatives for consideration.

The impact of privacy legislation on the Bill on the Data Processing by Partnerships Act

The Bill on the Data Processing by Partnerships Act (*Wet gegevensverwerking door samenwerkingsverbanden*; WGS) provides a legal basis for the systematic processing of personal data (including profiling) by partnerships.[125] These partnerships primarily involve cooperation between public-sector parties, and to a limited extent between public and private-sector parties.[126] The WGS covers partnerships that have a compelling interest in preventing and combating serious crime, the large-scale or systematic serious use of government funds and facilities, and the large-scale or systematic evasion of legal obligations to pay taxes, fees and duties on imports and exports. Partnerships included in the bill are the Financial Expertise Center (FEC), the Infobox for Criminal and Unexplained Assets (*Infobox Crimineel en Onverklaarbaar Vermogen*; iCOV), the Regional Information and Expertise Centers (RIECs) and the Care and Safety Houses.[127]

The bill is relevant to effective cooperation and combating serious crime, including financial and economic crime. This again shows the tension between fighting crime on the one hand, and privacy on the other. The Dutch DPA has issued several critical opinions and has called for the bill not to be passed in its proposed form.[128]

To summarize, the Dutch DPA's criticism amounts to the fact that the purpose partnerships have in sharing and processing personal data is not sufficiently clearly defined. The Dutch DPA also considers the timing of such sharing and processing to be too vague ('vague signals') and the categories of personal data are also too broad. Just as it did with the Bill on the Money Laundering Action Plan, the Dutch DPA speaks of the risk of '*unlimited surveillance*'.[129]

The foregoing demonstrates the tension between privacy regulations and protecting the integrity of the financial sector and preventing and combating financial and economic and other crime. What this means for gatekeepers and customers is further elaborated in the next section.

(123) Dutch Data Protection Authority, 'Nieuwe wet opent deur naar ongekende massasurveillance door banken', press release October 21, 2022; Dutch Data Protection Authority 2023.
(124) Dutch Data Protection Authority 2023.
(125) The current bill was passed by the House of Representatives on December 17, 2020, and is currently before the Senate for approval.
(126) Participation by private-sector parties is strictly limited to the private-sector parties currently participating in the FEC PPP: banks. The entry of new private-sector parties to regulated partnerships will be subject to a preliminary scrutiny procedure and a special subsequent scrutiny procedure before the Senate and the House of Representatives. See the consultation on the Data Processing by Partnerships Decree, February 20, 2023, available via this link; Senate, Memorandum of Reply on Rules on Data Processing by Partnerships, Parliamentary Papers I, 2022/2023, 35 447, K, pp. 22-23.
(127) In the WGS there is also the possibility of bringing other partnerships within the scope of the law.
(128) Dutch Data Protection Authority 2019c; Dutch Data Protection Authority 2019; Dutch Data Protection Authority, 'AP adviseert Eerste Kamer: neem WGS niet aan', press release November 9, 2021.
(129) Dutch Data Protection Authority, 'AP adviseert Eerste Kamer: neem WGS niet aan', press release November 9, 2021.

3.3 Implementation in practice and bottlenecks

Chapter 2 has shown that gatekeepers have been given great responsibility by the government in preventing money laundering and terrorist financing, and by extension in keeping the financial system 'clean'. The rationale behind making gatekeepers responsible is that money laundering and terrorist financing can be combated more effectively and efficiently by engaging the private sector than exclusively through the government.(130) This section outlines bottlenecks that impede effective and efficient compliance with anti-money laundering legislation. As a number of bottlenecks encountered by gatekeepers and customers stem from, or are related to, criticisms of the effectiveness of the anti-money laundering policy in general, this section begins by setting out some key criticisms.

3.3.1 Criticism of the effectiveness of the anti-money laundering policy

Research on the effectiveness of the anti-money laundering policy over the years paints a disappointing picture: money laundering and terrorist financing still seem to be a major problem despite more than 30 years of - expanding - policy.

Some common threads in the criticism of the effectiveness of the anti-money laundering policy can be found in the literature. These relate to (i) the separation of the anti-money laundering policy from the broader fight against (subversive) crime, (ii) the fact that money laundering is to a large extent an international phenomenon but is primarily combatted locally, (iii) the immeasurability of the effects of the policy, (iv) the imbalance between the roles and responsibilities of government and the private sector, and (v) the imbalance between gatekeepers' obligations and powers. These common threads are described in what follows.

1. Prevention of money laundering and terrorist financing vs combatting crime

One first criticism that emerges from the literature is that the anti-money laundering policy is disconnected, so to speak, from the broader fight against crime, and that this brings with it too narrow a focus.(131)

The cause seems to lie in the FATF's mandate, which is limited to combating money laundering, terrorist financing and the proliferation of weapons of mass destruction. As a result, the policy goals of the FATF - and, by extension, European and national anti-money laundering policies - are focused on the narrow idea of countering the activity of money laundering rather than on the higher, overarching goal of preventing crime.(132)

It is acknowledged - certainly in the Netherlands too - that the fight against money laundering and terrorist financing is closely related to the broader issue of subversive crime.(133) However, the legal frameworks, the parties involved, and the roles and responsibilities of these parties within the respective frameworks are different. This makes mutual coordination at policy level more complicated as more, and different, interests need to be represented. The aforementioned differences also complicate effective cooperation between parties on a practical level, as each party has its own (legal)framework for data collection and use. There is currently no overarching framework that ensures that parties can work together effectively and efficiently to achieve their own (and joint) statutory objectives.(134)

(130) Van Wingerde & Hofman 2022, p. 105; Alldridge 2016, pp. 13-14.
(131) Pol 2018, pp. 302-303; Reuter 2013, p. 224.
(132) Pol 2018, p. 303.
(133) One example is the broad deployment of ten Regional Information and Expertise Centers (RIECs) and the National Information and Expertise Center (*Landelijk Informatie- en Expertise Centrum*; LIEC) focusing on drugs crime, human trafficking and smuggling, criminal motorcycle gangs, real estate fraud, money laundering and financial and economic crime.
(134) In the 2021-2025 Coalition Agreement, *Looking out for each other, looking ahead to the future*, December 15, 2021, available via this link, the government, in its desire to strengthen the approach to tackle subversion, expressed its intention to draw lessons from the fight against the Mafia in Italy. This 'anti-Mafia strategy' is an integrated approach that includes the prevention of money laundering, creating a broad basis for information sharing between (public-sector) parties.

2. Money laundering is an international phenomenon; the fight takes place at local level

A second criticism concerns the fact that the actual fight against money laundering and terrorist financing mainly takes place locally. Although the FATF has issued global standards to combat money laundering, terrorist financing and the proliferation of weapons of mass destruction - and this policy was thus created with the intention of it becoming an international policy - each country has its own national framework due to the transposition of those standards. This means that, from a global perspective, the anti-money laundering policy is fragmented, or even '*an uneven playing field*'.(135) Money laundering is pre-eminently a global phenomenon that can only be effectively combated with a truly international approach.(136)

3. Immeasurability of the effects of the policy

There is also criticism about the immeasurability of the anti-money laundering policy. This criticism is directed both at the fact that the scope of the problem is not known - in other words: how much is being laundered? - and at the output side: what are the objectives of the policy and have these objectives been achieved?(137)

Although there are calculations of the scope of the money laundering problem, these are mostly just estimates.(138) In 2006, a study into the nature and extent of money laundering, commissioned by the Ministry of Finance, noted that most of the literature on the effects of combating money laundering is '*pure speculation*' and that empirical data is often lacking.(139) More recent publications still indicate that reliable estimates are lacking at both national and international level, and the recently published book 'The war on dirty money' still refers to calculations of the extent of money laundering as '*guesstimates*'.(140)

Furthermore, the lack of concrete, specific objectives in relation to protecting the integrity of the financial system and/or reducing crime contributes to the immeasurability of the policy's effectiveness.(141) Comparative research into the objectives of the anti-money laundering policy in the European Union also shows that different countries pursue different goals with their anti-money laundering policy.(142) The literature also points to the different objectives pursued by relevant parties with the anti-money laundering policy: public-sector parties focus primarily on catching criminals by following the money flows, while the private sector focuses on protecting the financial system and its reputation.(143) In the third study into the fight against money laundering, the Netherlands Court of Audit concluded that the Ministers of Finance and of Justice and Security still have "*a poor insight into the efficiency and effectiveness of their AML measures*" and that this is " *because the ministers have not stated precisely what they want the AML measures (...) to achieve.*"(144) The lack of measurable goals was also mentioned in the academic review of the recently submitted Bill on the Money Laundering Action Plan.(145)

4. Imbalance between the roles and responsibilities of the public and private sectors

Based on the idea of responsibility, gatekeepers have also been made partly responsible for what was originally a public task, shifting the focus of the anti-money laundering policy from the public to the private sector. However, investments made by the private sector in people and resources do not resonate down the chain. For example, there is a large discrepancy between the deployment of people and resources by gatekeepers compared to the public sector, and the outcome of the policy is also disproportionate to the resources put in at the front end.(146)

(135) Verhage 2017, p. 485.
(136) R. Betlem and M. Rotteveel, 'Machine tegen witwassen draait niet', *FD* January 10, 2023; RUSI 2018; 'The war against money laundering is being lost', *The Economist* April 21, 2021.
(137) Verhage 2017, pp. 478-479; Levi, Reuter and Halliday 2017; Zavoli and King 2021, p. 29.
(138) RUSI 2019, p. 15; Levi, Reuter and Halliday 2017, pp. 310 and 324.
(139) Unger et al. 2006, p. 102.
(140) Reuter 2013, p. 226; Levi, Reuter and Halliday 2017, p. 310; Gilmour and Hicks 2023, p. 49.
(141) See RUSI 2018; Amicelle 2017, p. 221.
(142) Unger et al. 2013, p. 27.
(143) Amicelle 2017, pp. 221-222.
(144) Netherlands Court of Audit 2022, p. 48.
(145) *Wetenschapstoets wetsvoorstel Plan van Aanpak Witwassen*, January 20, 2023, available via this link.
(146) Rakké and Huisman 2020, p. 10. See also, for example, H.W. Smits and H. Rasch, 'Anti-witwasbeleid kost miljarden en levert weinig op', *FTM* July 8, 2021; FD Editorial Comment, 'Banken voeren eenzame oorlog tegen witwassen', *FD* October 25, 2021.

In this regard, it should be noted that figures are difficult to translate and leave little room for nuance and contextualization.[147]

Nonetheless, to some extent this frustrates gatekeepers. In a KPMG study on how leaders deal with risk, one interviewee stated: "*The Wwft is truly an example of legislation for the stage. Each year there are 7,000 reports to the Financial Intelligence Unit, which are supposed to be reviewed by just 80 people. It completely misses its goal of combating money laundering and terrorist financing and this cannot be discussed with De Nederlandsche Bank.*"[148] On this point, a bank executive said in the same study: "*At our bank alone, there are more people working every day on compliance tasks to counter money laundering and terrorist financing than there are police officers walking the streets in the Netherlands. That makes you think.*"[149]

As an illustration, the DNB report 'From recovery to balance' already notes that, for the banking sector alone, the costs of combating money laundering and terrorist financing in 2021 totaled 8% of the total expenses of the four largest banks in the Netherlands. More specifically, this amounts to EUR 1.1 billion and over 10,000 FTEs. For the sector as a whole, these costs amounted to around EUR 1.4 billion in 2021, and the number of FTEs deployed was close to 13,000.[150] In contrast, FIU-NL - identified as playing a 'pivotal role in this system' "*because [FIU-NL] operates between the private-sector and public-sector parties*" - employed a total of 82 FTEs at the end of 2021 on a budget of EUR 9 million.[151] Incidentally, this information is somewhat dated: in 2023, approximately 100 FTEs were employed at FIU-NL and it is working toward increasing this number to approximately 130 FTEs over the year.[152] Looking at the end of the chain, the Public Prosecution Service's Annual Review Criminal Money Flows 2022 shows that in total just over EUR 246 million in criminal assets was seized in that year.[153]

The lagging results in the form of confiscated criminal assets compared to the costs and efforts of the private sector also come to the fore in international studies.[154] The Netherlands Court of Audit also notes this. In the study cited earlier, the Netherlands Court of Audit notes that "*the law enforcement agencies and the Public Prosecution Service cannot guarantee that disclosures with the highest risk will be investigated or prosecuted.*" The Netherlands Court of Audit then concludes that "*money laundering can (...) be combated more efficiently and effectively and more justice can be done to the efforts taken by private-sector parties(...)".*[155]

This discussion about roles and responsibilities and the division between the public and private sector, as well as the effectiveness of the anti-money laundering policy, does not only take place in the Netherlands. In response to the Parliamentary inquiry into the status of the UK anti-money laundering and sanctions regime in 2018, UK Finance (the trade association for the financial sector) argued that the current system invests too much in compliance activities that contribute little to detect criminals or protect customers. Moreover, the increased compliance and reporting obligations do not lead to an increase in the prevention of financial and economic crime.[156] According to UK Finance, the implemented anti-money laundering policy also affects financial institutions, in particular smaller parties and new entrants, which can hardly keep up with the speed of change and administrative burdens, and it states that "*[t]hese demands are exacerbated by the absence of prioritisation on competing demands from the public sector on economic crime resource within the financial sector. Firms also note that whilst the financial sector has increased resource on economic crime, there has been a reduction in public sector resource in this area.*"[157]

(147) See, for example, Public Prosecution Service 2022, p. 16, which states that "(...) published figures are often read without the necessary nuance". In this regard, the Public Prosecution Service refers to distinctions between transactions (reports) and files (composition of reports) and the fact that transactions are found suspicious on the basis of pre-existing 'proprietary investigation information'. The FIU Annual Review 2021 also reveals a clear difference between objective and subjective reports. Although objective reports are highly relevant as intelligence, transactions are declared suspicious to a far lesser extent (FIU 2021, pp. 7 and 10).
(148) KPMG 2022, p. 6.
(149) KPMG 2022, p. 25.
(150) DNB 2022, p. 15.
(151) Lagerwaard 2022, p. 147; FIU 2021, p. 32.
(152) Interview with FIU.
(153) Public Prosecution Service 2022, p. 8.
(154) RUSI 2019, p. 16, refers to estimates by UNODC and Europol.
(155) Netherlands Court of Audit 2022, p. 47.
(156) UK Finance 2018, pp. 1-2.
(157) UK Finance 2018, p. 2.

5. Imbalance between gatekeepers' obligations and powers

In the literature reference is made to the fact that the Wwft contains a broad obligation to carry out due diligence with corresponding obligations, but no powers.(158) Gatekeepers are expected to 'guard the gate', but they observe that the resources they have to do so are, in many cases, inadequate.(159) One interviewee for this study referred to this as "*guarding the gate with a cap pistol*".

In order to be able to fulfill their role as gatekeepers, they need powers. However, gatekeepers sometimes lack certain powers which would enable them to perform their duties properly, in particular for the increasingly onerous due diligence obligation that falls upon them. The recent FATF evaluation of the Netherlands, for example, shows that many gatekeepers have difficulty identifying UBOs because they do not have or cannot access suitable information. This is especially the case for complex (international) structures.(160)

> *"It feels like we are guarding the gate with a cap pistol"*

Statutory powers are mainly necessary when gatekeepers have to collect information which contains personal data or otherwise privacy-sensitive information.(161) Examples of powers that gatekeepers do not currently have but that they consider necessary for the performance of their gatekeeper function relate to the fact that most gatekeepers do not have access to the Personal Records Database (BRP) and that the UBO register is not widely accessible (and temporarily not accessible at all) to gatekeepers. The UBO register is an important source of information for gatekeepers, but also for parties that are exclusively subject to the Sanctions Act, like non-life insurers. Non-life insurers do not fall within the scope of the Wwft and use information from the UBO register in the context of due diligence under the Sanctions Act and the RtSw 1977.(162)

Prior to the UBO register being closed in its entirety as a result of the European Court of Justice ruling(163), gatekeepers only had access to the public section of the register, even though the closed section also contained relevant information for gatekeepers.(164) This included, for example, the date and place of birth and the residential address of UBOs.(165) The lack of a search function by name in the Business Register is also a thorn in the side of several gatekeepers.(166) Sometimes laws and regulations *are* in the pipeline, but often this takes months or even years. One example is the Central Shareholders Register: the proposed bill dates from 2017 and in 2023 it is still pending in the House of Representatives.(167) Again, access to the UBO register was mentioned by interviewees as an example. Since the UBO register was closed, gatekeepers have been awaiting emergency legislation that could give them access again. The Cabinet has indicated that it will submit the emergency legislation to the House of Representatives around the summer, more than six months after the European Court of Justice's ruling.(168)

Specifically with respect to the Sanctions Act, it is noted that sanctions lists are not always complete, which can sometimes lead to institutions having to put disproportionate efforts into determining the structure and control of a particular relationship in order to comply with the Sw. It has therefore been suggested that a public-sector party or criminal investigation service could carry out the due diligence on the structure and UBO/control. The results of that due diligence could possibly lead to additional listings, on which institutions could then rely.(169)

(158) Nuijten 2023, p. 144.
(159) See also Hoogenboom 2021, pp. 39-40; Nuijten 2023, p. 144.
(160) FATF 2022b, pp. 126 and 129.
(161) Nuijten 2023, p. 144.
(162) Dutch Association of Insurers, 'Meer duidelijkheid toegang UBO-register', news release January 24, 2023.
(163) Court of Justice of the EU, November 22, 2022, C-37/20 and C-601/20, ECLI:EU:C:2022:912 (*WM v Luxembourg Business Registers* and *Sovim v Luxembourg Business Registers*).
(164) Nuijten 2023, p. 145.
(165) NVB 2019; Hoogenboom 2021, p. 40.
(166) Hoogenboom 2021, p. 40.
(167) See Senate, *Initiatiefvoorstel-Nijboer en Alkaya Wet centraal aandeelhoudersregister*, available via this link.
(168) On May 30, 2023, the consultation on the Restriction of Access to UBO Registers (Amendment) Act started, available via this link.
(169) Hoff and Hoff 2023, p. 11.

The lack of possibilities to share information about (joint) customers with other gatekeepers is also perceived as a limitation.[170]

Finally, interviews conducted as part of this study indicate that gatekeepers do not feel that they have the leeway to be able to rely on work that other gatekeepers have already carried out, even though this is legally permissible (i.e. the introductory customer due diligence).[171] Gatekeepers have indicated that it requires so much effort to be able to demonstrate that they can rely on the policies and processes of the introducing institution that it is more efficient to carry out the customer due diligence themselves.

The imbalance in gatekeepers' obligations and powers - or the lack of adequate powers in light of the expanded due diligence obligation - also specifically results in some of the bottlenecks gatekeepers encounter. These are discussed in the section below.

3.3.2 Bottlenecks encountered by gatekeepers

Gatekeepers have been assigned a role and responsibility in safeguarding the integrity of the financial sector but - as the foregoing shows - the effectiveness of all the efforts contributed to actually preventing financial and economic crime cannot be determined. This means that support for complying with the obligations is not a given.[172] Broadly speaking, the implementation of the gatekeeper role encounters four bottlenecks, which are outlined in this section. These are the tension between commercial interests and the gatekeeper function, conflicting laws and regulations, limited government support and the fact that the gatekeeper role has been put under a magnifying glass.

1. Divergent interests

There is tension between the commercial interests of private-sector parties, including their customer relationships, on the one hand, and the public interest in contributing to the prevention of financial and economic crime on the other.[173] These interests are closely intertwined: large fines imposed by regulators and reputational damage have an impact on commercial results. This tension is referred to by Van Wingerde and Hofman as 'the existential split'.[174] Research shows that the commercial interest plays an important role in gatekeepers' decisions to report unusual transactions. The tension between commercial interests and the prevention of financial and economic crime often comes to the fore in internal discussions between 'the business', where the commercial interest prevails, and organizations' compliance departments.[175] In addition to the public interest in the prevention of financial and economic crime, gatekeepers also have to deal with societal expectations. For instance, banks are increasingly expected to contribute actively to broad-based social ambitions in areas such as sustainability, climate, environment, health, human rights and governance.

The tension between commercial interests on the one hand, and the implementation of the gatekeeper role - sometimes supplemented by societal expectations - on the other, applies in principle to all gatekeepers.[176] Commercial pressures can be perceived as greater by small gatekeepers, because they are more dependent on a smaller group of customers or have to compete more with larger parties and usually have relatively fewer financial and human resources to implement the Wwft.[177] The trade-off between commercial and public interests also has an impact on investments made to be Wwft-compliant. The administrative burden and the costs of complying with the Wwft are perceived by gatekeepers to be enormous, and these are continuing to rise as obligations increase.[178]

(170) Parliamentary Papers II, 2022/2023, 36 228, no. 3, p. 4. See also Wolfsberg Group 2022, p. 1.
(171) Section 5(1) Wwft.
(172) Van Wingerde and Hofman 2022, p. 16.
(173) Van Wingerde and Hofman 2022, p. 16; Rakké and Huisman 2020, p. 8; Stichting Maatschappij en Veiligheid 2022, pp. 33-34.
(174) Van Wingerde and Hofman 2022, p. 67.
(175) Rakké and Huisman 2020, pp. 8-9.
(176) Yeoh 2020; Van Wingerde and Hofman, p. 69; Hoogenboom 2021, p. 39.
(177) Van Wingerde and Hofman 2022, p. 69; EY 2021, p. 47.
(178) Hoogenboom 2021, p. 40; Zavoli and King 2021, p. 26.

Moreover, because of the risk-based approach and the associated open standards, it is not always clear in advance whether an institution has sufficient personnel and technological resources (in terms of quality and quantity) to detect irregularities. Commercial pressures are also perceived to be a bottleneck for information sharing between gatekeepers, namely if information sharing is perceived as giving a competitive advantage to the other party because it reveals which customers a party is serving, or if one of the two parties carries out the customer due diligence and incurs the associated costs.(179)

Research by Nyenrode Business University shows that support for the Wwft and the gatekeeper role is increasing among real estate agents/appraisers and civil-law notaries.(180) At the same time, key provisions of the Wwft are still not always complied with properly. Researchers speak of the 'rebellious commitment'(181) of individual professionals and cite commercial interests as one of the causes. Researchers argue that there are gray areas "*in which the contexts of the business relationships, the deal and the commercial interests vary. Depending on those changing contexts, decisions are made that are not always driven by the normativity of the Wwft.*"(182) Other causes can be found in the (perceived) complexity of the Wwft and other regulations and the lack of adequate powers to fulfill the gatekeeper role.(183) Conflicting laws and regulations and the supporting role of the government are discussed later on in this section.

Although there is no known literature that addresses the tension between gatekeepers' commercial interests and compliance with the Sanctions Act, parallels with the Wwft can possibly be drawn here to some extent. Compliance with the Sanctions Act also entails a certain obligation to carry out due diligence - and thus incur costs; particularly for gatekeepers that have to comply with the RtSw 1977 and that are subject to supervision.

Here too, fines and other forms of enforcement by the regulator can have an impact on commercial results and/or reputation.

2. Conflicting laws and regulations

Another bottleneck relates to the existence of conflicting interests between different laws and regulations or in relation to the professional responsibility of the different gatekeepers. For instance, civil-law notaries are, in principle, obliged to carry out work arising from the law, the so-called 'duty to provide services'.(184) Refusal is only allowed if, according to the civil-law notary's reasonable belief or suspicion, the work is contrary to the law or to public order, if his cooperation in acts that manifestly have an unauthorized purpose or effect are required, or if he has other justifiable reasons for refusing.(185) However, the true purpose of the service cannot always be ascertained, which means that the line between having to provide notarial services and ceasing to provide services based on suspicions of money laundering is vague.(186)

A broader conflict between the legislation pertaining to some professionals and the Wwft, concerns the confidentiality and secrecy in the customer relationship. Confidentiality is absolutely fundamental to the professional practice of attorneys, civil-law notaries and accountants and, in a derivative form, it may also apply to tax advisors. This confidentiality may be at odds with the openness and transparency required for recording data and reporting unusual transactions under the Wwft.(187) Confidentiality is also at odds with (European)sanctions obligations. Owing to this duty of confidentiality, the decision that has currently been taken was not to impose a reporting obligation on the notarial, legal and accountancy professions.(188)

(179) Maxwell 2021, p. 9.
(180) Hoogenboom 2021, p. 64.
(181) Hoogenboom 2021, p. 37.
(182) Hoogenboom 2021, p. 64.
(183) Hoogenboom 2021, pp. 110-111.
(184) Van Wingerde and Hofman 2022, p. 75.
(185) Section 21(2) of the Notaries Act.
(186) FATF 2022b, p. 128; Van Wingerde and Hofman 2022, p. 75.
(187) Van Wingerde and Hofman 2022, p. 16.
(188) National Coordinator for Sanctions Compliance and Enforcement 2022, p. 13.

The Netherlands has asked the European Commission to break this confidentiality obligation for the purpose of a sanctions reporting obligation. As part of the modernization of the sanctions system, the possibility of regulating this at national level is also being explored.(189) Gatekeepers who, at the same time, are also 'keepers of confidentiality', experience a dilemma when they have to apply confidentiality on the one hand but have a reporting obligation on the other, both prompted by their roles and responsibilities.(190) Professional confidentiality also clashes with the desire to exchange more information within the profession and with other gatekeepers in the context of combating financial and economic crime.(191)

"There is currently a privacy lock on fighting crime in the Netherlands"

There is an inherent tension between privacy and combating money laundering and terrorist financing as well. In this context, the FATF states that both represent an important public interest: "*both serve important objectives, including upholding human rights and fundamental freedoms (such as the right to privacy) and protecting the public from criminal activities, including terrorism. These interests are not in opposition nor inherently mutually exclusive.*"(192) The FATF states that an effective anti-money laundering policy presupposes that the public and private sectors comply with both the requirements of the anti-money laundering regulations and the privacy regulations. Privacy legislation, and in particular the role of the Dutch Data Protection Authority in the public debate in the Netherlands, were also frequently cited in interviews conducted as part of this study as a major factor limiting the implementation of the Wwft. In one interview, interviewees stated that "*there is currently a privacy lock on fighting crime in the Netherlands*".

The tension between protecting the privacy of citizens and businesses on the one hand, and fighting crime effectively on the other, is clearly evidenced in the case of the Bill on the Money Laundering Action Plan, which actually aims to increase the effectiveness of the Wwft through increased information exchange, as elaborated in section 3.2.5.

There is also tension between the duty of care that financial institutions have under the Financial Supervision Act (Wft) and compliance with the Wwft.(193) In order to keep integrity risks manageable or to fulfill societal expectations or their own ambitions in the areas of sustainability, climate, environment, health, human rights and governance, financial institutions decide to refuse some or all customers with a higher risk profile or to provide limited services.(194) However, under the general duty of care, in some cases they cannot refuse or terminate the relationship because the consequences would be disproportionate for the customer. This could be the case if the customer cannot find an alternative and would be denied access to the payment system if the relationship were to be terminated. This especially applies to natural persons, who have the right to a bank account.(195) Case law shows that refusing to provide or terminating services because of risks of money laundering and terrorist financing can be at odds with the duty to provide access to the financial sector.(196)

Recently, the National Coordinator against Discrimination and Racism stated that banks and financial institutions structurally discriminate against Muslims as a result of the application of the Wwft.(197) Gatekeepers are expected to carry out risk-based due diligence and to identify and report unusual transactions. In doing so, they process information about customers and transactions. Institutions may also request further information in the context of complying with the Sanctions Act.(198)

(189) National Coordinator for Sanctions Compliance and Enforcement 2022, p. 13; Letter from the Minister of Foreign Affairs on the status of sanctions compliance, its supervision and enforcement: Parliamentary Papers II, 2022/2023, 36 045, no. 120, p. 3; Hoff and Hoff 2023, p. 8.
(190) On the relationship between confidentiality and Wwft obligations see: Van Wingerde and Hofman 2022, pp. 72-73.
(191) Ipenburg 2023, p. 27.
(192) FATF 2022, p. 3.
(193) Nuijten 2023, p. 145.
(194) NVB 2022a, p. 15.
(195) This is the basic checking account pursuant to Section 4:71f Wft. To date, no such right exists for legal entities.
(196) See, for example, Appellate Court of Amsterdam, January 21, 2020, ECLI:NL:GHAMS:2020:121; District Court of Amsterdam, January 5, 2022, ECLI:NL:RBAMS:2022:42; District Court of Amsterdam, June 15, 2022, ECLI:NL:RBAMS:2022:3871; District Court of Amsterdam, September 14, 2022, ECLI:NL:RBAMS:2022:5340.
(197) 'Racismecoördinator: 'Structurele discriminatie van moslims bij banken', *NOS.nl* April 6, 2023, NVB, 'Openheid en transparantie in uitvoering anti-witwaswet', news release April 6, 2023.
(198) See, for example, the Netherlands Institute for Human Rights, 'Verzoek geweigerd – Mogen banken klanten afwijzen op grond van nationaliteit?', news release April 4, 2023.

Finally, real estate agents encounter another conflict in laws and regulations. Under the Dutch Civil Code, real estate agents are prohibited from engaging in two-way representation, that is to say: to act on behalf of both the buyer and the seller.[199] At the same time, the real estate agent has an obligation to carry out due diligence on the business relationship and the (real estate) transaction. In order to be able to assess whether a transaction is unusual or not, or whether a transaction is used to circumvent sanctions, real estate agents need to carry out due diligence on the counterparty. In view of the potential harm to the negotiating position, counterparties are often reluctant to provide the necessary information about the amount and origin of their own funds in practice.[200] Also, when the buyer and seller each have their own real estate agent, this leads to the situation that both real estate agents involve each other's customers in their own customer due diligence. In doing so, the due diligence is duplicated. The guidance from the Dutch Tax Administration/Wwft Supervision Office indicates that real estate agents can outsource the due diligence on the counterparty to the civil-law notary (if the civil-law notary is drawing up the deed of sale) or to the real estate agent's own customer, although that brings with it a potentially higher risk which requires additional measures to be taken by the real estate agent. When multiple real estate agents are involved, the guidance indicates that the real estate agents may outsource the respective customer due diligence on the counterparty to each other.[201]

3. Limited government support

In a system where increasing value is placed on the gatekeeper function carried out by private-sector parties, it is also important for the government to enable those same gatekeepers to carry out their role effectively and efficiently. In this study, a supportive government means a government that creates appropriate enabling conditions for gatekeepers to carry out their duties. From interviews conducted as part of this study, it appears that gatekeepers do not feel adequately supported at present by the government, which has assigned them the gatekeeper role. The government increasingly expects more from them, making it a challenge for gatekeepers to fulfill their role effectively. The imbalance between gatekeepers' obligations, powers and responsibilities has already been mentioned in this study (section 3.3.1), but the fragmentation and lack of prioritization of government policies and a lack of guidance and feedback also fuel this feeling of the private sector.

Fragmentation and a lack of prioritization of public policies

Gatekeepers deal with lots of different government parties: within the anti-money laundering policy, the sanctions regulations, and the broader approach to organized crime.[202] In the Netherlands, these include various ministries (e.g. the Ministry of Finance, the Ministry of Justice and Security, the Ministry of the Interior), Wwft regulators, other regulators like the Dutch Data Protection Authority and the Netherlands Authority for Consumers and Markets, FIU-NL, the Public Prosecution Service and criminal investigation services (the police, FIOD, the Royal Netherlands Marechaussee), government services (Customs Administration of the Netherlands), municipalities and other bodies with governmental tasks (the Netherlands Cadastre, Land Registry and Mapping Agency and the Netherlands Chamber of Commerce). All these parties have their own task in combating subversive and/or financial and economic crime, and thus have their own interests to promote. A picture emerges from the interviews that there is a lot of trying to reach consensus between these parties and their interests. As a result of this fragmentation on the government side, there is no clear ownership or steering of the anti-money laundering and sanctions policies.[203] Priorities are not set or communicated unambiguously to the private sector.[204]

The lack of clear ownership and direction is a bottleneck that goes up to the highest level of government.

(199) Article 7:427 in conjunction with Article 7:417 of the Dutch Civil Code.
(200) Hoogenboom 2021, p. 41.
(201) Dutch Tax Administration/Wwft Supervision Office, *Leidraad Wwft voor makelaars, bemiddelaars en taxateurs onroerende zaken*, March 2022, available via this link, p. 39.
(202) Verhage 2017, p. 480, calls this the '*AML complex*'; Hoff & Hoff 2023, p. 7.
(203) RUSI 2019, pp. 19-20; National Coordinator for Sanctions Compliance and Enforcement, 2022, p. 15.
(204) This problem is not limited to the Netherlands. It has also been noted in the UK that the anti-money laundering policy in the UK is "*underpowered, poorly coordinated*" and that it lacks strategic oversight and vision: RUSI 2018.

Interviews conducted as part of this study reveal that there isa clearly shared desire for the government to make a clear choice between privacy and the fight against crime and that it will have to accept that assigning greater importance to one interest means limiting the other. Until that choice is made, no steps or only limited steps will be able to be taken in reducing money laundering, terrorist financing and other crime.

Lack of guidance and feedback

Gatekeepers feel the need to get a better understanding of the actual biggest threats to the integrity of the financial sector. Governments are required to identify, analyze, understand and mitigate money laundering and terrorist financing risks and need to keep their risk assessments up to date.(205) For the most part, governments do this through National Risk Assessments (NRAs). Research shows that NRAs are still at an early stage: "*they lack conceptual clarity, the data are highly limited, most are analytically weak or fail to explain the methodology, and the whole goal of the NRA - to inform policy decisions - is often missed or at least not made explicit in the published version.*"(206) Others argue that, in part because of their generic nature, NRAs are of little use as a basis for a risk-based anti-money laundering policy.(207) Interviews with various gatekeepers suggest that the Dutch NRAs do not currently provide enough specific guidance for gatekeepers. For instance, they find that risks are said to be present in entire sectors or activities, without there being an indication of where the risks really lie or how money can be laundered through them. Other interviewees indicated that the NRA is a learning process and that it should indeed include more details; at the same time, they pointed to the role of gatekeepers in providing information that could improve the NRA.

There is also a need for coordinated guidance from and continuous dialogue with the Wwft/Sw regulators, for example on shared topics where multiple gatekeepers are involved (e.g. real estate) and in which situations can be clearly discussed; for instance where, from a risk perspective, more effort is expected of gatekeepers and, in particular, where less effort is possible and allowed.(208) That last point seems to be the most important; interviews reveal that, although risk-based standards on paper lead to fewer rules, gatekeepers often do more in practice than is strictly necessary because it is not clear in advance when the effort compared to the risk has been met or what the regulator is expecting specifically.(209)

Having an ongoing dialogue between gatekeepers and regulators on adequate risk assessment and management is considered a valuable addition to the ex-post supervision of gatekeepers.(210) In this regard, DNB's 2022 initiative to organize roundtable discussions, with banks and other industries affected by anti-money laundering measures, on the risk-based approach of the Wwft and the use of innovative means can be seen as a positive development.(211) The first five NVB Standards were published in May 2023 based on these roundtable discussions.(212)

Furthermore, the literature and interviews conducted as part of this study show that gatekeepers need an effective feedback loop from FIU-NL, criminal investigation services and regulators.(213) This feedback loop is important for organizations to be able to learn and to increase the quality of their reports. A lack of feedback can affect gatekeepers' motivation to report.(214)

(205) FATF Recommendation 1 and Article 7 AMLD5. This obligation has been implemented in Section 1f Wwft. Under the Wwft, the Dutch NRA must be updated every two years.
(206) Ferwerda and Reuter 2022, p. 22.
(207) Gilmour and Hicks 2023, pp. 132-133.
(208) See, for example, Zavoli and King 2021, pp. 26 and 28.
(209) Nuijten 2023, p. 145. See also further on in this section.
(210) NVB 2022a, p. 24.
(211) DNB, 'Partijen voortvarend van start met gerichte risicogebaseerde witwasaanpak', news release November 23, 2022.
(212) NVB, 'Minder klantimpact door NVB Standaarden voor risicogebaseerd witwasonderzoek', press release May 30, 2023. The NVB Standards were created in consultation with regulator De Nederlandsche Bank (DNB) and the Ministry of Finance.
(213) Rakké and Huisman 2020, Van Wingerde and Hofman 2022, Zavoli and King 2021, p. 42, Netherlands Court of Audit 2022, p. 32, Stichting Maatschappij en Veiligheid 2022, p. 32, FATF 2022b, pp. 121, 123 and 140; Wolfsberg Group 2022, p. 1; Verhage 2017, p. 482.
(214) Rakké and Huisman 2020, p. 11.

In the Annual Review Criminal Money Flows 2022, the Public Prosecution Service reports that it is working with FIOD, FIU-NL and the police, within the Suspicious Transaction (*verdachte transactie*; VT) Working Group, on: "*better file transfer of VTs to investigation, more insight in use and usefulness of VTs, enhancing the feedback loop and better chain cooperation.*"[215] In the first half of 2023, the banking sector also joined this working group.

Another bottleneck related to making reports to FIU-NL is the fear of retaliation. When reports of unusual transactions by gatekeepers lead to, or are included in, criminal proceedings, the name and other details of the reporting institution become known to the defendant, through inclusion of these details in the criminal file. The literature, as well as interviews conducted as part of this study, suggests that this can deter gatekeepers from making important reports for fear of being targeted by the underworld, especially when combined with the hardening of organized crime.[216] Some measures have already been taken with respect to this since 2020. FIU-NL only makes the name of the organization available to the criminal investigation service when an unusual transaction is declared suspicious. The criminal investigation services always contact reporters when they intend to place a report in the criminal file, to determine whether there are certain risks of threats to the reporter. The reporter can also file a report with the police or contact the police. In exceptional cases, the data in the criminal file is anonymized. Nevertheless, the group of 'small' gatekeepers, in particular, continues to perceive this as a bottleneck, interviews reveal. There is a feeling that where gatekeepers have a government-imposed duty to report, that same government has a duty to protect reporters.

In May 2023, in response to Parliamentary questions, the Minister of Justice and Security announced that she would be exploring various solutions to enhance the safety and the sense of safety of reporters.[217]

In this regard, the Minister indicated that "*it is also important, in addition to exploring additional measures to enhance safety and the sense of safety among gatekeepers, to communicate even better about, among other things, the usefulness and importance of the reporting obligation and the safeguards that are already in place.*"[218]

4. The gatekeeper role under a magnifying glass

The imbalance between powers and obligations combined with the perceived limited government support is further exacerbated by the risk of gatekeepers being dealt with harshly themselves when, in the opinion of that same government, they fail to fulfill their gatekeeper role, or fail to do so adequately.[219] This relates to both administrative or disciplinary law enforcement by regulators and to criminal enforcement by the Public Prosecution Service. Without having been directly involved in money laundering or terrorist financing, there have been cases where gatekeepers have been criminally prosecuted for not fulfilling their gatekeeper role properly.[220] According to Nuijten, this creates the impression "*that the special and general preventive effect of punishing gatekeepers is considered greater than that of punishing money launderers.*"[221]

A related relevant development also concerns the increased focus on the role of directors: based on the regulations, there is increasing focus on the quality and responsibilities of directors (both individually and collectively) as well as on other key individuals in the anti-money laundering policy of gatekeepers.[222]

(215) Public Prosecution Service 2022, p. 15.
(216) Hoogenboom 2021, pp. 39 and 136; K. van Doorne, 'Met knikkende knieën ongebruikelijke transacties melden? Dat kan toch niet', *VNO-NCW* column, April 5, 2023.
(217) Parliamentary Papers II, 2022/2023, Appendix to the Proceedings, 2595.
(218) Parliamentary Papers II, 2022/2023, Appendix to the Proceedings, 2595, p. 7.
(219) This is done by both Wwft/Sw regulators and the Public Prosecution Service. Examples include administrative and disciplinary law enforcement by regulators, as well as the Public Prosecution Service's settlements with ING and ABN AMRO, prosecutions of or deals with gatekeepers for the failure to report unusual transactions (e.g. District Court of Amsterdam, April 22, 2021, ECLI:NL:RBAMS:2021:2600; Appellate Court of The Hague, February 1, 2019, ECLI:NL:GHDHA:2019:187; Public Prosecution Service, 'Trustkantoor Vistra betaalt 3,5 ton voor niet melden ongebruikelijke transacties', news release September 3, 2019). See also: AMLC, *Strafrechtelijke aanpak via de Wwft*, available via this link.
(220) Van Wingerde and Hofman 2022, p. 13; Daalderop 2019, p. 50; Nuijten 2023, p. 144.
(221) Nuijten 2023, p. 144.
(222) Nuijten 2023, p. 144; Zwinkels 2020. That last article examines how realistic it is for compliance officers to face administrative or criminal penalties too. Although this has not yet occurred, the author, citing cases abroad, concludes that it would not be out of the question for DNB and the Public Prosecution Service to be able to and to go on to use their powers against compliance officers.

This includes, for example, the developments around fit and proper assessments, and specific requirements that ensue from the EBA guidelines.[223] In the context of enforcement, it is also increasingly being considered whether directors - possibly in addition to the Wwft institution itself - can also be personally prosecuted in the event of non-compliance or insufficient compliance with the Wwft.[224] This increases the - already high - pressure on institutions and their directors even further.

A recent interview with top executives from the Public Prosecution Service and VNO-NCW in the FD also revealed that prosecuting directors "*creates a lot of turmoil in boardrooms.*"[225] The Public Prosecution Service believes that prosecuting gatekeepers is still important: "*[w]here possible, we will look at crimes under ordinary criminal law, but we know from experience that from an evidential point of view, often only crimes that fall under the Money Laundering and Terrorist Financing (Prevention) Act/Economic Offences Act can be prosecuted.*"[226]

This approach toward gatekeepers results in a situation where gatekeepers become tensed up and feel compelled to do more than necessary, which is also referred to as the 'rule-based' implementation of risk-based standards or as 'compliance-oriented' adherence, just to make sure that they can demonstrate compliance with all the requirements.[227] This tensing up manifests itself in directors becoming resistant to taking risks; these are avoided because avoiding negative scenarios has become the status quo.[228] On this point, a bank director stated the following in a KPMG study: "*[E]veryone supports a good gatekeeper function for banks, but it is incredibly difficult for any bank to act in accordance with the spirit of the law in doing so. Actually, following the letter of the law is the easiest option. Then you do not get into trouble and you do not get negative press as a result either, but from a social point of view that does not benefit anyone.*"[229] This tensing up and fear of mistakes also translates into the implementation of the gatekeeper role in the workplace. Interviews reveal that gatekeeper employees involved in day-to-day Know Your Customer/Customer Due Diligence (KYC/CDD) processes need clear frameworks and instructions.

Compliance-oriented adherence manifests itself, in particular, in the context of gatekeeper reporting behavior. The result is that reports are made with the idea of 'covering' the institution against any possible legal consequences of not reporting. Compliance is then the driver for reporting, rather than the prevention of financial and economic crime. This is also referred to as 'defensive reporting' or the 'crying wolf' problem and results in many low-quality reports being made to FIU-NL.[230] This input has implications for the rest of the anti-money laundering chain: scarce resources have to be devoted to analyzing those reports and they do not contribute to preventing money laundering and terrorist financing either.[231]

3.3.3 Bottlenecks encountered by customers

Customers, both individuals and companies, are also encountering bottlenecks in gatekeepers' implementation of the Wwft. Some of the bottlenecks encountered by customers mirror those encountered by gatekeepers. As there is, however, a difference in perspective, we have nevertheless chosen to address these bottlenecks in this section as well. These include reduced access to the financial system, processing times and costs, and repeated and unnecessary queries. This section looks at these three bottlenecks from the customer's perspective.

(223) For example, European Banking Authority, *Guidelines on the role and responsibilities of the AML/CFT Compliance Officer*, EBA/GL/2022/ 05, June 14, 2022, available via this link.
(224) Examples include the criminal prosecution of former ING CEO Hamers and the designation of several former directors as suspects in a criminal investigation by the Public Prosecution Service into ABN AMRO.
(225) M. Pols, E. van der Schoot, 'OM-topman: 'Ik mis de verontwaardiging over criminaliteit die het bedrijfsleven ondermijnt'', *FD* April 21, 2023.
(226) Public Prosecution Service 2022, p. 17.
(227) DNB 2022, pp. 20-21; RUSI 2019, pp. 19-20; Stichting Maatschappij en Veiligheid 2022, pp. 35-36; Hoogenboom 2021, pp. 180-181. See also Michael Levi and Tom Keatinge in KPMG 2022a, pp. 28 and 32.
(228) KPMG 2022, p. 4.
(229) KPMG 2022, p. 25.
(230) Unger and Van Waarden 2013; Takáts 2007; Amicelle 2017, p. 219; Vogel 2022, p. 53. Takáts makes an analogy for excessive reporting to the ancient Greek fable 'The boy who cried wolf'. In the book, the boy makes it seem as though a wolf keeps attacking his sheep so that when it actually happens, no one listens to him and he gets eaten.
(231) UK Law Commission 2019, p. 31; Gilmour & Hicks 2023, p. 128.

1. Reduced access to the financial system

Partly due to increased regulatory pressures and limited supportive role from the government, combined with pressure from regulators and the Public Prosecution Service, gatekeepers are increasingly scrupulous about whether or not they can and will accept and mitigate certain risks. Based on a risk analysis, gatekeepers can decide on a case-by-case basis whether to provide services to a customer. The gatekeepers' weighing up of the costs and benefits of implementing the Wwft and the Sw can lead to them not or no longer providing or wanting to provide services to certain customers.(232) Individuals and companies with higher integrity risks, for instance customers from industries where a lot of cash is in circulation, associations or foundations, or customers who have been designated as a PEP, may find themselves being refused services or only being provided with limited services.(233) The same supposedly applies to certain population groups, as the National Coordinator against Discrimination and Racism stated.(234) When there is exclusion of a certain category of customers or a restriction on them, this is called 'de-risking'.(235) A study by the European Banking Authority (EBA) reveals that de-risking can have a negative impact on combating financial and economic crime, on promoting financial inclusion, and on competition and stability on the financial markets.(236) DNB also notes that unnecessary de-risking can potentially "*undermine the effectiveness of the Wwft while also eroding support for compliance with the legislation. Supervision may be similarly affected.*"(237) Interviews conducted as part of this study confirm the view that certain groups of entrepreneurs and businesses are having difficulties opening a bank account. This is notably also true of gatekeepers themselves: in recent years, there have been several lawsuits about the termination of relationships with trust offices.(238) The FATF also addressed this in its evaluation of the Netherlands, labeling it a cause for concern.(239)

2. Long processing times, increase in costs and the administrative burden

Customer due diligence costs time and money, and customers are experiencing long processing times before the services start.(240) When customers belong to a segment with heightened integrity risks, due diligence is even more time-consuming and expensive. These additional costs are increasingly being passed on to customers.(241) Estimates by the Dutch Banking Association (*Nederlandse Vereniging van Banken*; NVB) and PwC suggest that costs for a business bank account are increasing by up to EUR 2,000.(242) Between 2018-2022, the average cost of banking increased by 42%, partly due to the money laundering perspective, according to the banks.(243) On top of this, customers often face additional costs themselves due to the complexity and volume of information requested.(244) In one of the interviews conducted as part of this study, interviewees indicated that companies and businesses quite often have to hire external advisors to meet information requests from gatekeepers.

3. Repeated and unnecessary queries

Both individuals and businesses have to deal with different gatekeepers at different points in time. To illustrate this, we follow the customer journey of the owner of a small or medium-sized business and of an individual. This shows that customers have to deal with multiple gatekeepers, both when conducting a single transaction in the same time frame (e.g. when buying real estate) and over a longer period of time (e.g. when expanding a business).

(232) NVB 2022a, p. 13.
(233) See, for example, R. Betlem, 'Rabobank sluit kleine autodealers uit vanwege risico op witwassen', *FD* July 1, 2021; Goede Doelen Nederland, *Tweede brandbrief aan Kaag over gevolgen de-risking banken*, April 21, 2022, available via this link; 'Banken weigeren goede doelen om 'witwasrisico', *RTL Nieuws* November 15, 2022; 'ING te druk met witwasonderzoek, weert stichtingen en verenigingen', *NOS.nl* August 29, 2022. As of June 1, 2023, it is again possible for foundations and associations to open a new account, according to the ING website.
(234) 'Racismecoördinator: 'Structurele discriminatie van moslims bij banken', *NOS.nl* April 6, 2023. In addition, see section 3.3.2 on conflicting laws and regulations.
(235) DNB 2017, p. 8.
(236) EBA 2022, p. 2.
(237) DNB 2022, p. 22.
(238) For example, District Court of Amsterdam, December 1, 2020, ECLI:NL:RBAMS:2020:6245; District Court of Amsterdam, January 5, 2022, ECLI:NL:RBAMS:2022:42.
(239) FATF 2022b, p. 121.
(240) NVB 2022a, p. 14; R. Vaessen, 'Even een rekening openen', *Accountant.nl* September 6, 2019.
(241) R. Betlem, 'Zakelijke rekeningen duurder door stijgende kosten witwasonderzoek', *FD* August 30, 2022.
(242) NVB 2022a, p. 14.
(243) P. de Waard, 'Kosten voor bankrekening blijven stijgen, ABN AMRO gooit er in een keer 51,3 procent bovenop', *Volkskrant* May 3, 2022; 'Bedrijven, stichtingen en kerken moeten van banken meebetalen aan witwasonderzoek', *NOS.nl* December 27, 2022.
(244) NVB 2022a, p. 14.

As each gatekeeper is required to have its own information and customer file, customers keep having to provide (more or less) the same data to each individual gatekeeper.(245) Gatekeepers are also required to redo their customer due diligence during the course of the relationship, which in turn can lead to customers receiving repeated queries.

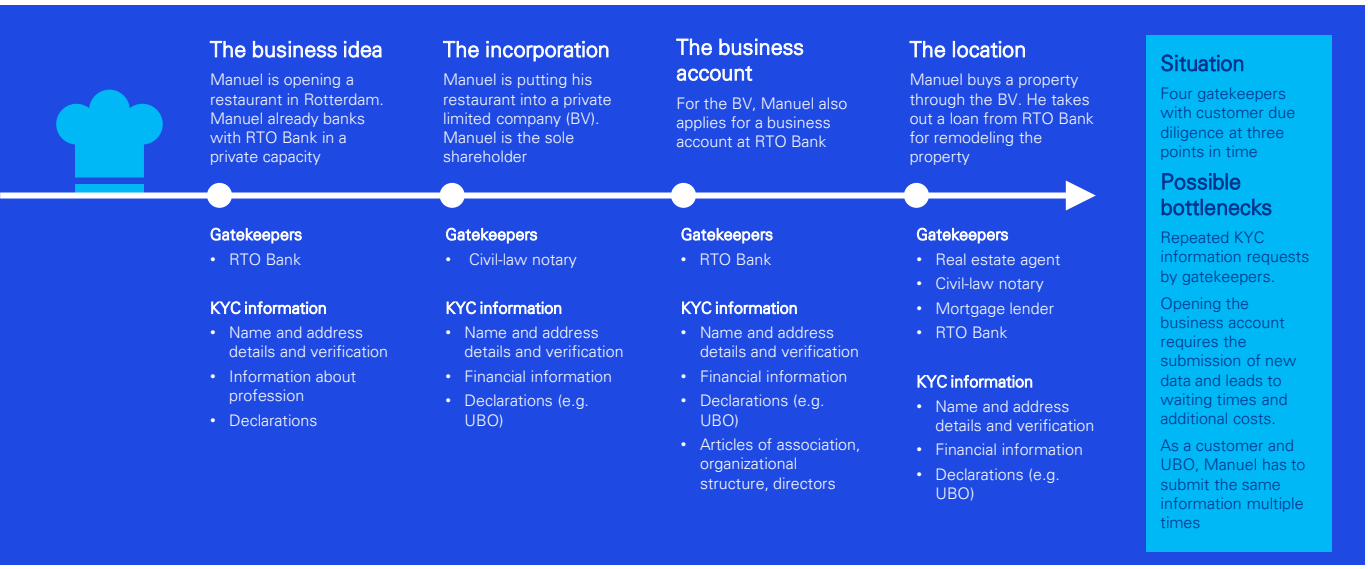


Figure 2: Customer journey of the owner of a small or medium-sized business

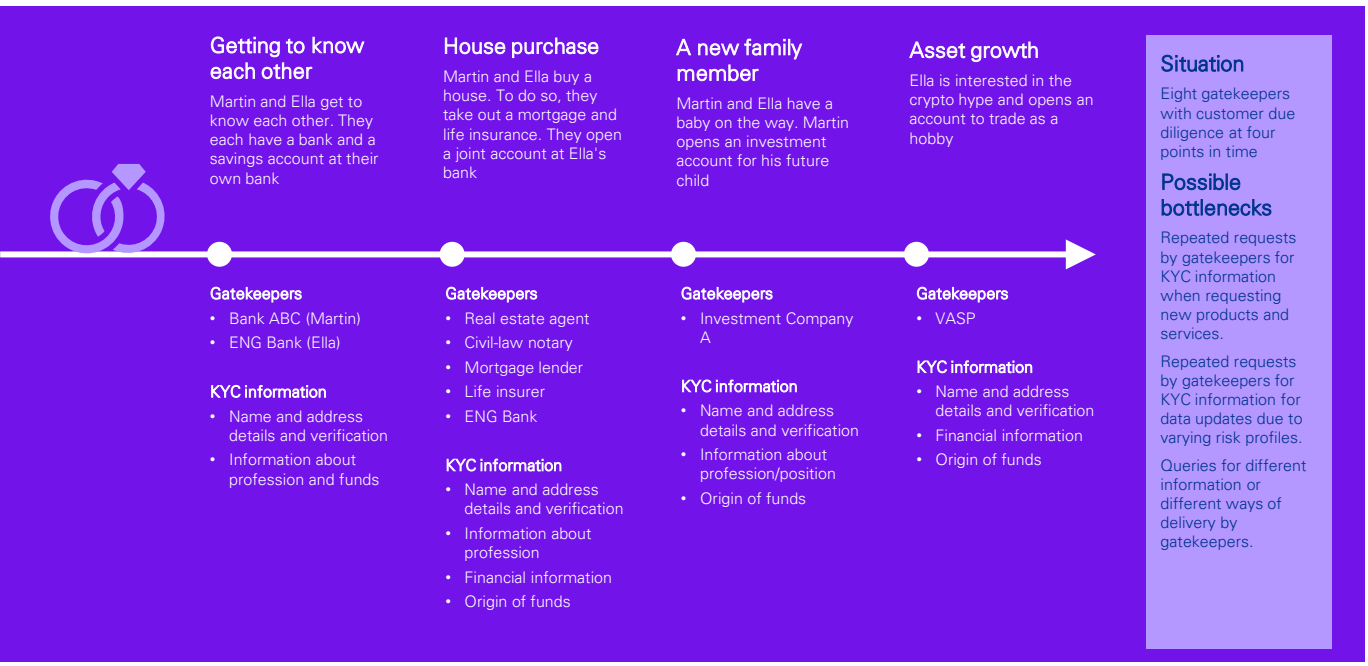


Figure 3: An individual's customer journey

Previous research and interviews conducted as part of this study show that customers are annoyed by the repeated provision of data, especially if the information is the same or similar.(246) In the report 'From recovery to balance', DNB indicates that it has received reports suggesting that customers feel like banks are requesting unnecessary information, or information they would rather not share.(247)

(245) RUSI 2019, p. 20.
(246) NVB 2022a, p. 13.
(247) DNB 2022, p. 21. See also Maxwell 2020, p. 9.

3.3.4 Bottlenecks identified by regulators and the Public Prosecution Service

The publicly available Wwft enforcement decisions of the AFM and DNB, and the disciplinary complaints of the Financial Supervision Office (*Bureau Financieel Toezicht;* BFT) against civil-law notaries, show that gatekeepers are breaching various Wwft standards.[248] Breaches range from inadequate or entirely no risk assessment or systematic integrity risk analysis[249] to the unjustified failure to conduct enhanced customer due diligence[250], inadequate monitoring of transactions[251], and the failure to report unusual transactions or to report them in a timely manner[252]. It is not only core obligations that are being breached. The enforcement decisions and disciplinary complaints also reveal alleged breaches due to the lack of an independent compliance function[253], outsourcing (Section 10)[254], the retention obligation (Section 33 Wwft)[255] and the training obligation (Section 35 Wwft)[256].

Whereas regulators' enforcement decisions tend to be technical in nature and focused on proving breaches, criminal investigations and settlements by the Public Prosecution Service provide a more in-depth view on the causes of identified breaches. In 2018, ING Bank reached a settlement with the Public Prosecution Service for "*gross negligence in preventing money laundering.*"[257] In 2021, ABN AMRO Bank reached a settlement with the Public Prosecution Service for the same allegation.[258]

Both statements of facts and conclusions - known as 'Houston' and 'Guardian', respectively - detail how the corporate culture, the tone at the top, and poor communication and corporate organization played a role in the Wwft breaches.[259] Some of these (organizational) cultural bottlenecks include:

- Inadequate tone at the top and insufficient focus on and priority given to the anti-money laundering policy. It is clear from the statement of facts and conclusions in Houston that in the case of ING Bank there was insufficient awareness among senior management of the importance of complying with the Wwft and thus the tone at the top did not convey this adequately.[260] In order to achieve effective compliance with legal obligations, conveying the right tone at the top is important.[261] The findings in the ING Bank case are not isolated: research indicates that compliance departments experience opposition from senior management in carrying out their duties.[262]
- Culture. In the case of ABN AMRO Bank, the Public Prosecution Service argued that non-compliance with the Wwft also stemmed from the culture. According to the Public Prosecution Service, the state of affairs was presented in a better light than was actually the case, giving the idea that problems could be solved in a 'business as usual' way.

(248) The Dutch Tax Administration/Wwft Supervision Office website only shows administrative sanctions against car dealers (until 2021). No public enforcement decisions for Sanctions Act violations have been published by DNB and AFM because the regulators do not have this power under the 1977 Sanctions Act.
(249) AFM, *Aanwijzing Zwaan Finance B.V.*, March 25, 2022, available via this link; AFM, *Bestuurlijke boetes Revo Capital Management B.V.*, May 25, 2022, available via this link; DNB, *Aanwijzing MUFG Bank (Europe) N.V.*, July 29, 2019, available via this link; DNB, *Bestuurlijke boete Suri-Change B.V.*, November 25, 2014, available via this link; AFM, *Bestuurlijke boete Robeco Institutional Asset Management B.V.*, March 31, 2022, available via this link.
(250) See, for example, AFM, *Aanwijzing STX Fixed Income B.V.*, June 8, 2021, available via this link; Amsterdam Division for Notarial Matters, March 10, 2022, ECLI:NL:TNORAMS:2022:8; The Hague Division for Notarial Matters, July 15, 2022, ECLI:NL:TNORDHA:2022:14; Den Bosch Division for Notarial Matters, September 19, 2022, ECLI:NL:TNORSHE:2022:31; CBb, October 18, 2022, ECLI:NL:CBB:2022:707 (Bunq).
(251) See, for example, AFM, *Bestuurlijke boete Robeco Institutional Asset Management B.V.*, March 31, 2022, available via this link; DNB, *Bestuurlijke boete Suri-Change B.V.*, November 25, 2015, available via this link; CBb, October 18, 2022, ECLI:NL:CBB:2022:707 (Bunq).
(252) DNB, *Bestuurlijke boete JTC Institutional Services Netherlands B.V.*, June 14, 2021, available via this link; DNB, *Bestuurlijke boete Travelex N.V.*, February 2, 2023, available via this link; AFM, *Bestuurlijke boete FlatexDeGiro*, December 23, 2021, available via this link; Den Bosch Division for Notarial Matters, September 19, 2022, ECLI:NL:TNORSHE:2022:31; The Hague Division for Notarial Matters, July 15, 2022, ECLI:NL:TNORDHA:2022:14; AFM, *Bestuurlijke boete Robeco Institutional Asset Management B.V.*, March 31, 2022, available via this link.
(253) See, for example, The Hague Division for Notarial Matters, May 25, 2022, ECLI:NL:TNORDHA:2022:10 (disciplinary complaint declared unfounded) and CBb, March 3, 2020, ECLI:NL:CBB:2020:120.
(254) Rabobank, *Rabobank has received a draft instruction from DNB*, November 16, 2021, available via this link.
(255) See, for example, AFM, *Aanwijzing STX Fixed Income B.V.*, June 8, 2021, available via this link; Rabobank, 'Rabobank has received a draft instruction from DNB', press release November 16, 2021.
(256) See, for example, AFM, *Aanwijzing Zwaan Finance B.V.*, March 25, 2022, available via this link; AFM, *Aanwijzing STX Fixed Income B.V.*, June 8, 2021, available via this link.
(257) Public Prosecution Service 2018.
(258) Public Prosecution Service 2021.
(259) Public Prosecution Service 2018, p. 13; Public Prosecution Service 2021, pp. 21-22.
(260) Public Prosecution Service 2018, p. 13.
(261) See also David Lewis in KPMG 2022a, p. 35.
(262) Rakké and Huisman 2020, p. 11.

- Business before compliance. There was inadequate investment in systems and staff capacity because of commercial objectives. The statement of facts and conclusions in Guardian reveals that although apparently 'money was not a problem', there was actually no budget available. This finding refers back to the aforementioned bottleneck encountered by gatekeepers in the tension between the commercial interest and the gatekeeper role.
- Poor internal organization. Both statements of facts and conclusions reveal that the three lines of defense did not function well, that the organization was set up in a way that caused compartmentalization/siloing, that indications did not reach senior management, and that communications were inadequate. This created a limited overview of the actual extent of non-compliance and an overview of the remedial actions needed was also lacking.

The Public Prosecution Service's findings in these cases are not isolated. In an analysis of the involvement of banks in some money laundering scandals carried out by the European Commission, the Commission also noted that the failure to adequately fulfill the gatekeeper role can be traced back to structural governance problems. In this regard, the Commission mentioned the poor functioning of the three lines of defense and the internal reporting and escalation processes, the culture in which commercialism prevailed and the fact that senior management was insufficiently informed.(263)

3.4 Concluding remarks on the implementation of the Wwft and the Sanctions Act

The implementation of the Wwft and the Sw is being affected by various legislative developments. What is striking is that especially developments surrounding the Wwft and the Wtt are moving very quickly.

Developments are also currently taking place in the area of sanctions. With society's increasing focus on privacy and the Dutch DPA's active role, which is often critical, in the public debate on combating crime, including money laundering and terrorist financing, that tension is also coming to the fore. Technological developments like artificial intelligence, the digital identity and wallet and blockchain are also affecting the implementation of the Wwft and Sw; these could play a positive role in effective and efficient compliance with the Wwft and the Sw. Of course, it is important to be mindful of safeguards around privacy and cybersecurity, for example, with these developments.

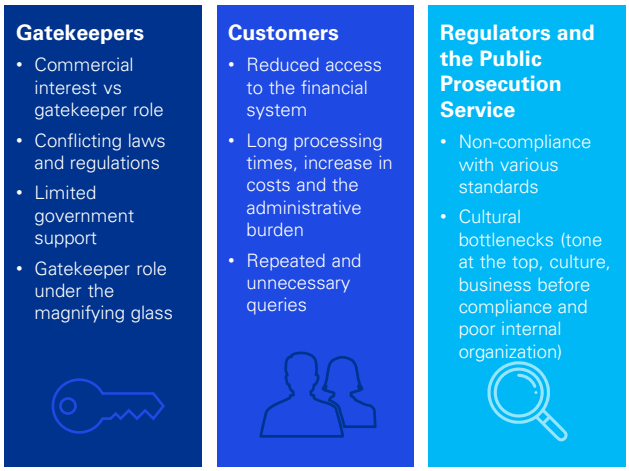


Figure 4: Summary of bottlenecks encountered by gatekeepers, customers and regulators

Figure 4 shows the identified bottlenecks in implementing the Wwft and the Sanctions Act in practice. It is notable that the bottlenecks encountered by gatekeepers and customers, and those identified by regulators and the Public Prosecution Service, can be traced back to a number of fundamentals of the anti-money laundering policy.

(263) European Commission 2019, pp. 4-5. See also: Yeoh 2020.

There seems to be a vicious circle where clear policy goals are lacking, clear central coordination is missing or is at least perceived to be so, and expectations about the respective roles between, and efforts made by, the public and private sectors are mutually divergent. The imbalance between gatekeepers' obligations and powers also plays a role.

Regarding the gatekeeper role, it has been noted that there are tensions between the commercial raison d'être of the gatekeepers and the fulfillment of their gatekeeper role, and that in several areas they feel like they have insufficient support from the government at the front end, for example through clear direction and prioritization, guidance and feedback. This can cause frustration and is detrimental to their motivation as gatekeepers to 'guard the gate' well. If they do not, this in turn requires government efforts at the back end in the form of various types of enforcement. At the same time, enforcement information shows that non-compliance by gatekeepers is not solely due to the aforementioned reasons. The consequences of the vicious circle can be seen in the bottlenecks encountered by customers: financial exclusion and increased costs. All bottlenecks together lead back to the - as yet unanswerable - key question of the anti-money laundering policy: to what extent are money laundering and terrorist financing actually prevented?

Deepdive into initiatives in the Netherlands and abroad

4

4.1 Introduction

In light of the research question and the identified relevant developments and bottlenecks from the previous chapter, a deepdive was conducted into initiatives undertaken in the Netherlands and abroad that could serve as possible solutions or alternatives for improved effectiveness and efficiency of compliance with the Wwft and the Sw. This involved looking at preconditions, success factors and lessons learned that are being taken into account in developing possible solutions in this study.

The deepdive conducted for this study shows that lines of thought for possible solutions or alternatives need to be sought primarily in **technology** and **collaboration**. In summary, these are the following lines of thought:

1. The main point is the ability for gatekeepers to share information. This may involve, for example, the development of private partnerships or utilities, often with the main purpose of making customer due diligence and/or ongoing monitoring more efficient.(264) It may also involve the use of warning systems to improve the effectiveness of customer due diligence conducted by gatekeepers and to keep the financial system 'clean'.(265) Various aspects such as technology (e.g. distributed ledger technology and blockchain technology), privacy protection and legal (im)possibilities on information sharing play an important role and also affect the degree of success of initiatives that are being developed in the Netherlands and abroad.
2. A second point here is the development and use of digital identity - also called 'digital ID wallets' ('wallets') or 'financial passports'. This is attracting a great deal of attention in the Netherlands and abroad. It is also briefly explained in section 3.2.4 as a relevant technological development.(266) There are already several commercial and other initiatives in the Netherlands and abroad, but their use in the context of customer due diligence seems to be at an early stage. Depending on the design, partnerships between private-sector parties such as the utilities and the use of digital identity may run together, but this need not be the case.(267)
3. A third point is that public-private partnerships are seen as a means of increasing the effectiveness of preventing money laundering, terrorist financing and compliance with sanctions regulations, the idea being that financial and economic crime can be better reduced by working together and sharing knowledge and intelligence.

   In its evaluation of anti-money laundering policies in the Netherlands, the FATF praised domestic collaboration in both public-public and public-private partnerships and even called it a '*key feature*' of the Dutch system.(268) Chapter 3 has shown that an effective feedback loop and a balance between private-sector input on the front end and output in the form of criminal convictions and seizures by the public sector are essential in this regard.
4. Chapter 3 also demonstrates a clear need for a more centralized government, one that speaks more with one voice, makes clear choices and sets priorities. Bottlenecks such as fragmentation of government policy, conflicting laws and regulations, and a perceived lack of guidance and feedback can be traced back to this issue. This also applies to the bottlenecks experienced by customers. Consequently, this point was also included in the deepdive for this study.

The following sections elaborate on these lines of thought. Selected initiatives from the Netherlands and abroad are discussed on the basis of each of these lines of thought.

(264) BIS 2023, pp. 12-13.
(265) On KYC utilities and information sharing between private-sector parties, see *inter alia* FATF 2017; T. Lyman and L. de Koker, 'KYC Utilities and Beyond: Solutions for an AML/CFT Paradox', *CGAP Blog Series Beyond KYC Utilities* 1 March 2018; Zetzsche et al. 2018; CGAP 2019; FATF 2022.
(266) See, for example, Zetzsche et al. 2018; Leung et al. 2022; DNB 2022.
(267) Zetzsche et al. 2018. See Annex B for MyInfo service on Singpass, where there appears to be a confluence.
(268) FATF 2022b, p. 52.

The detailed analyses of these initiatives are described in Annex B to this report. The initiatives were selected with a view to obtaining a balance between new and old(er) ones, successful and less successful ones, and ones with shared characteristics but also each with their differences. A number of focus areas or lessons learned were identified for each theme. The insights gained can be incorporated into the development of possible solutions in response to the present research question.

4.2 Information sharing between gatekeepers

4.2.1 Joint utilities and 'gray' lists

"*It takes a network to defeat a network.*"[269] Forming networks, partnerships and collaborations - both private-private and public-private (see section 4.4) - is increasingly being seen as the way to act more effectively and efficiently in the fight against money laundering, terrorist financing and underlying crime by organized criminal organizations.[270]Effective information sharing is cited by the FATF as one of the cornerstones of an effective anti-money laundering policy.[271]

Mutual sharing of information at the typology and customer level produces deeper knowledge to start with. It enables gatekeepers (and also public-sector parties in the case of public-private partnerships) to better fulfill their role. For example, they can use the shared information to better assess the risks of both potential and actual customers or monitor business relationships with greater focus. Secondly, it can improve the quality of unusual transaction reports.[272] Thirdly, sharing information about joint customers can also enhance the efficiency and customer-friendliness of customer due diligence. Customers often deal with more than one gatekeeper, and sharing customer information between them can reduce the number of repeated requests for information, cut costs, lessen administrative burdens and produce faster turnaround times.[273] The main effect of this for customers is less inconvenience and it also enables gatekeepers to use their limited resources elsewhere.

"It takes a network to defeat a network"

Several countries are experimenting with information sharing between gatekeepers. These initiatives are mostly driven by or for banks. Joint facilities, also called joint utilities, where information about customers and/or their transactions is shared, can focus on both the CDD process and ongoing monitoring in the form of transaction monitoring or sanctions screening.[274] The so-called transaction monitoring utilities (TM utilities) primarily have the potential to provide the parties concerned with a 'broader' picture than just the transaction involving them and thus to discover unusual or suspicious patterns of behavior that would otherwise go undetected.[275] Based on research, the Bank for International Settlements (BIS) states that "*[u]tilising network analysis for detecting anomalous and suspicious networks shifts the focus from individual behaviour to the overall behaviour of suspicious networks, resulting in improved detection capabilities.*"[276] The BIS concludes that "*[t]he main findings of Project Aurora suggest that behavioural-based transaction monitoring and analysis at national or international levels is more effective in detecting money launderers and suspicious networks than current siloed and rule-based monitoring.*"[277] TM utilities appear to be especially relevant to gatekeepers with considerable transaction flows and sustained business relationships, such as banks, payment service providers, crypto service providers and trust offices.

(269) U.S. General Stanley McChrystal apparently said these words at the decisive stage in the war against IS in Iraq.
(270) RUSI 2017; FATF 2017; FATF 2022; RUSI 2022; KPMG 2022a; BIS 2023.
(271) FATF 2017, p. 2.
(272) FIU 2023, p. 2.
(273) KPMG 2018, p. 3.
(274) BIS 2023, pp. 79; A. Clare, 'Sanctions screening regtech GSS secures $45mn in funding', *Fintech Magazine* January 23, 2023.
(275) FATF 2022, p. 3; NVB 2022, p. 3; NVB 2023, p. 5; BIS 2023, p. 74.
(276) BIS 2023, p. 13.
(277) BIS 2023, p. 74.

Well-known examples of collective transaction monitoring initiatives are Transactie Monitoring Nederland B.V. (TMNL), the TriBank pilot in the United Kingdom and COSMIC in Singapore.[278] TMNL as well as its potential to improve effectiveness and efficiency in detecting possible unusual transaction patterns are detailed in Annex B. Joint utilities based on aspects of CDD - also referred to as 'KYC utilities' abroad and in the literature - mostly aim to improve the efficiency of customer due diligence by gatekeepers through the repeated use of data (data circularity) and the ability to update and optimize it (data mutualization).[279] There are many such joint utility initiatives in the Netherlands and abroad, a selected number of which are detailed in Annex B. These initiatives show varying degrees of success: some initiatives have recently been discontinued, while others have yet to start or have just begun.

Another form of information sharing among gatekeepers involves developing a warning system. A warning system can enable gatekeepers to operate more effectively by being aware of incidents and/or risks surrounding natural persons or legal entities. Such information puts them in a better position to assess the risks of a (prospective) customer during the customer due diligence process and take actions to mitigate any risks.

Unwanted 'shopping behavior' can also be prevented.[280] From a privacy perspective, it is important to look at the safeguards that should accompany such a system.[281] It is also important that being listed in a registry does not imply a *de facto* refusal or termination of a business relationship.[282] In the Dutch context, the Incident Warning System for Financial Institutions is an example found in the financial sector. Details of this warning system can be found in Annex B to this report.

4.2.2 Overview of information sharing initiatives between gatekeepers

Figure 5 shows some of the information sharing initiatives used by gatekeepers as well as their status. Red initiatives are ones that have been stopped; orange initiatives are under development or are operating subject to restrictions (e.g. awaiting legislative or regulatory changes) and green initiatives are active. For this deepdive, a number of initiatives with different statuses were examined to understand relevant aspects and lessons learned.

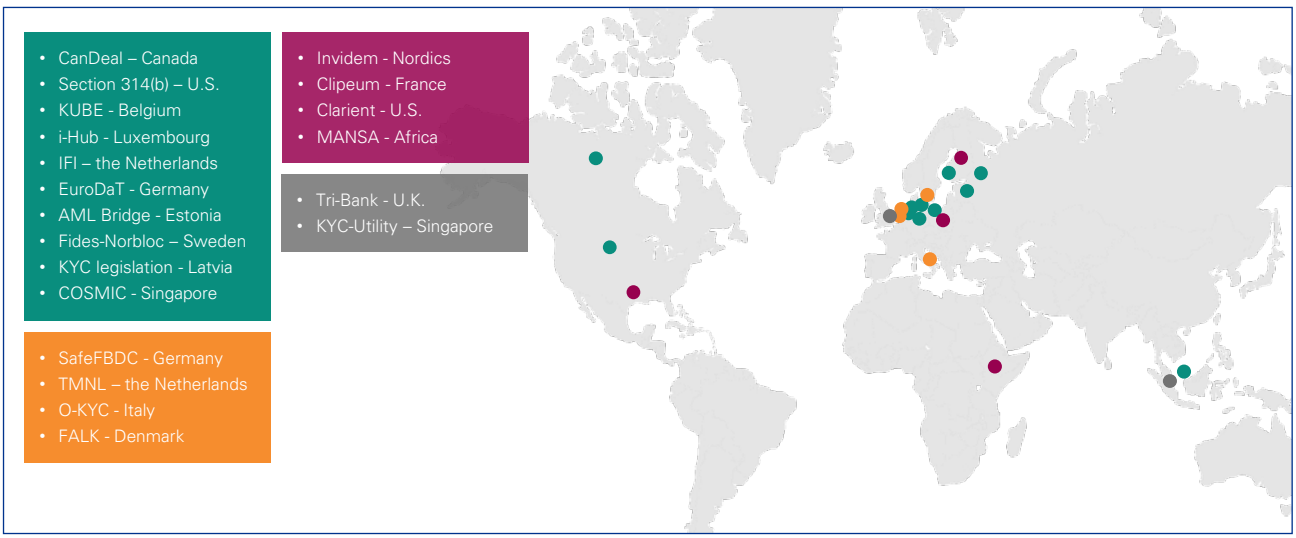


Figure 5: Overview of information sharing initiatives worldwide

(278) See FATF 2022, pp. 20-22 (Tribank pilot) and 22-26 (COSMIC).
(279) KPMG 2018, p. 7.
(280) In this regard, see also the Bill on the Money Laundering Action Plan (*Wet plan van aanpak witwassen*) and the accompanying Explanatory Memorandum, introducing an inquiry obligation for institutions subject to the Wwft: Parliamentary Papers II, 2022/2023, 36 228, nos. 2 and 3. For trust offices, this is already an obligation under Section 68 Wtt 2018.
(281) Berkvens 2011, pp. 210-214.
(282) RUSI 2022, p. 36.

4.2.3 Insights gained from domestic and foreign initiatives

Insights based on joint utilities and 'gray' lists

Around the world, private partnerships and utilities are being experimented with, with varying degrees of success. In the wake of pilots and projects, benefits that can be gained from private partnerships and utilities are being pointed out, however. One of these is the shortening of customer due diligence and a corresponding decrease in costs. Available data is reused, so to speak, and it is constantly updated and enriched (data circulation and data mutualization).(283) At the same time, this eliminates the need for addressing repeated queries to customers. As regards TM utilities, another point to note is that network analyses are able to glean more information than an individual bank could. For example, the added value in increasing the quality of unusual transaction reports has already been pointed out by FIU-NL in the context of TMNL.(284) A possible improvement in the efficiency of the transaction monitoring process, reduced costs due to the joint development and maintenance of utilities, and improved risk management have also been pointed out.(285)

The joint utilities analyzed in this deepdive show that they have all been set up and/or are being managed by private-sector parties; the government's role in them is purely supportive, e.g. amending (or changing the interpretation of) laws and regulations or providing opportunities for experimentation. What also emerges is that there is a difference between the types of joint utilities in terms of CDD: where some utilities are really 'by and for' the gatekeepers - with or without the support of a platform operator (KUBE, Invidem, O-KYC and a closed shared KYC utility in Latvia) - other utilities are in fact services provided by commercial service providers to whom gatekeepers can outsource all or part of their CDD work (i-Hub KYC and the open shared KYC utility in Latvia).(286)

Several initiatives have been discontinued (prematurely) in the past, and the initiatives involved in this study are also in different stages. As regards a number of initiatives that were stopped or paused or did not move beyond the pilot phase, reference is made to the fact that the subject-matter proved to be technically and operationally far more challenging than initially thought; another factor was the impossibility of achieving the desired economies of scale.(287)

Setting up a utility and getting it operational is therefore no easy task. It is clear from the initiatives and the literature that several aspects need to be carefully considered. These include:

- Technology: what technology platform is being used? Is the preference for a centralized or a decentralized platform? There are advantages and disadvantages to both types. For example, it is sometimes said that the advantage of a decentralized platform is that participants are in better control of the data and the risks from a cybersecurity perspective are lower. In that regard, the initiatives seem to have a preference for decentralized platforms.(288) Frequently cited technologies are Distributed Ledger Technology (DLT) and blockchain technology. However, other technologies are not ruled out: there is no one solution that will meet all needs, regardless of country, regulatory framework or size of institution.(289) There is also the cost issue involved in centralizing all data: for example, the KYC Utility project in Singapore, which was discontinued in 2018, noted the high cost of migrating data to a central platform.(290)

(283) Intesa, 'Progetto O-KYC, inizia la fase due', press release dated October 5, 2022.
(284) FIU 2023.
(285) BIS 2023, p. 80.
(286) For details of the initiatives mentioned, refer to Annex B.
(287) ABS 2018, p. 1; M. Ciobanu, 'Interview Advancing modern financial crime prevention with KYC utilities – interview with Invidem', *ThePaypers* June 25, 2021.
(288) Zetzsche et al. 2018, p. 140; N. Twomey, 'KYC Utilities: The Second Coming, Learning from Past Failures', *Finextra Blog* November 13, 2017; ABS 2018, p. 7.
(289) KPMG 2018, p. 6: *"(…) it is important to note that there is no one solution that will meet all needs, regardless of country, regulatory environment or size of institution."*
(290) ABS 2018, p. 7.

- Participants: given the current costs of setting up a utility, the size of the customer portfolio and the degree of automation of customer processes, it is not surprising that most of the initiatives are undertaken in the banking sector. For each utility, consideration will need to be given to the intended participants: are they financial and/or non-financial institutions, is the utility limited to a particular sector or not, and can it be of added value in specific areas, e.g. real estate? The participants will also need to have trust in each other and a willingness to share information among themselves.(291)
- Type of information and actualization: careful thought will have to be given beforehand to what information is to be shared. Current initiatives show that this can include information coming from the parties involved themselves, as well as public information and information from government registers such as the UBO register. It will also be necessary to consider how often the information will be updated and by whom. This also raises questions around liability for anything that goes wrong and how to deal with 'supplying' and 'receiving' participants.(292)
- Types of customers: different approaches were observed in the initiatives studied: some initiatives target corporate customers, others individuals. Setting up a CDD utility for corporate customers is more complex than for, say, 'mass retail' customers (e.g. this involves investigating their organizational structure and UBOs, multiple representatives and directors); however, it could potentially be more beneficial to participants in terms of reduced costs and shortened turnaround times if customer due diligence can be standardized. Careful consideration will need to be given in advance to which customers will come under the scrutiny of the utility.
- Functions of the utility: a joint utility can have several functions. It could be purely a channel through which existing information is routed, or it might also have a role in validating the data shared through it. The i-Hub KYC Repository for Ongoing Due Diligence even shows that the KYC utility can also play a role in customer risk assessment. Depending on the desired functions, consideration could also be given to whether customer contact might perhaps be conducted by a KYC utility, e.g. obtaining the customer's permission to share their information through the utility or requesting them to provide current information.
- Data standardization: what standards are to be used for sharing data? Will each participant determine its own standard or is the aim to develop a harmonized standard? It turns out that institutions regularly request different information, even where the same laws and regulations apply. The Invidem initiative as well as the KYC-Utility project in Singapore both show that a shared data standard or taxonomy, along with good data quality, is considered essential for successful information sharing.(293) Data standardization is also important for TM utilities.(294)
- Governance: governance is fundamental to joint utilities. This involves several questions: is it better for the utility to be a private-sector party or a public-sector party? Should it be a for-profit or a not-for-profit organization? Who manages the joint facility on a daily basis? Do the participating parties have participatory or voting rights? How are new members admitted and who decides that?(295) Again, the question arises as to who is liable if anything goes wrong.

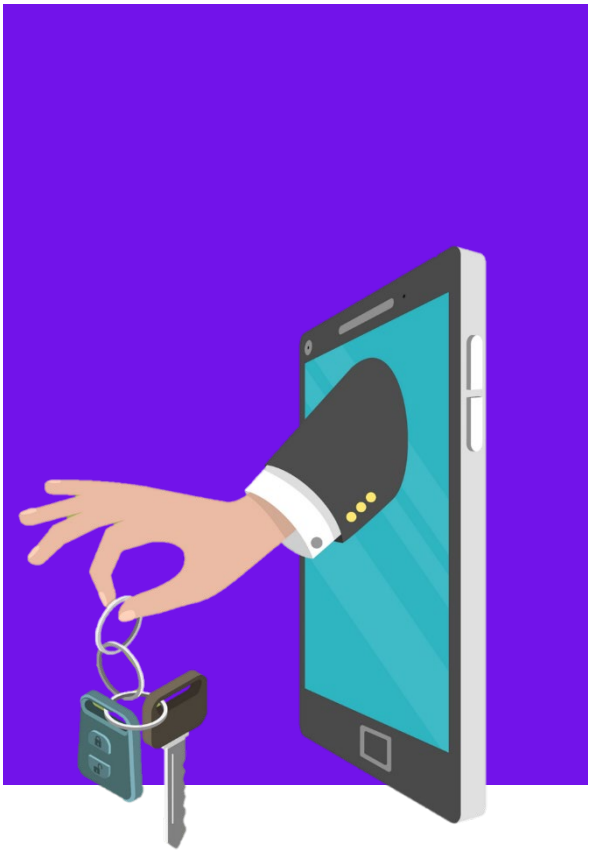
(291) BIS 2023, p. 80.
(292) ABS 2018, p. 6.
(293) M. Ciobanu, 'Interview Advancing modern financial crime prevention with KYC utilities – interview with Invidem', *ThePaypers* June 25, 2021; ABS 2018, p. 4; N. Twomey, 'KYC Utilities: The Second Coming, Learning from Past Failures', *Finextra Blog* November 13, 2017; Zetzsche et al. 2018, p. 141.
(294) BIS 2023, p. 80.
(295) See also Zetzsche et al. 2018, p. 142.

Looking at Latvia and Luxembourg - which mainly involve (gatekeeper) independent service providers - it may still be relevant for the governments to assess whether to introduce a licensing regime, with or without oversight by, for example, a privacy regulator.

- Privacy: The design and operationalization of a joint utility should not be considered solely from the perspective of combating financial and economic crime. Data sharing carries risks in several areas, particularly privacy. It has also been said in this regard: "*Knowledge is power, and where there is a lot of knowledge, there is a lot of power.*"[296] The initiatives show that privacy can be included in a variety of ways. In TMNL, for example, data is pseudonymized. Several other initiatives rely on the consent principle: the customer determines who may (no longer) see what data. The initiatives also use other privacy-enhancing measures, such as data minimization and the appointment of a privacy officer.[297]
- Intellectual property, competition, cybersecurity: these aspects should also be considered when developing a KYC utility. Another important factor is who is responsible for these aspects and who oversees them.
- Collaboration with the government: several initiatives interact with governments. A clear 'lesson learned' from the KYC Utility project in Singapore is that a joint utility has little chance of success without the existence of intensive public-private partnerships.[298] The report on the KYC Utility project refers to the cooperative approach taken by public-sector parties in the search for the sources ('golden sources').[299] Government collaboration is also important where there is the need to amend or interpret laws and regulations. BIS also emphasizes the importance of collaboration between the private sector and government when developing utilities.[300] The Dutch DPA's critical stance on the banks' joint transaction monitoring in the context of TMNL once again confirms the importance of good collaboration with the government: a collaboration that should come from both sides.[301]

By extension, it is also crucial for government to speak with one voice and to dare to make a clear trade-off between conflicting (or potentially conflicting) interests.[302]

- Cost: finally, it should always be borne in mind that choices made in relation to the above elements have an impact on costs, such as utility start-up and ongoing (operational) costs. The balance between costs and benefits also needs to be monitored continuously. Another important consideration is who will bear the costs and whether sustainable financing for utilities can be guaranteed.



(296) Zetzsche et al. 2018, p. 142.
(297) See also BIS 2023, pp. 48-63.
(298) ABS 2018, p. 6.
(299) ABS 2018, p. 5.
(300) BIS 2023, pp. 14 and 72.
(301) See section 3.2.5 of this report, which sets out the critical stance of the Dutch Data Protection Authority ("Dutch DPA").
(302) RUSI 2022, p. 95.

Key lessons for establishing a joint utility based on initiatives

Some important lessons can be drawn from existing utility initiatives:

1. Start small and let the initiative grow.

- *Limit the number of participants initially*: effectiveness and efficiency are important factors and are best achieved when as many parties as possible participate. At the same time, developing a joint utility involves many aspects and it becomes increasingly difficult to agree on them when more parties participate.
- *Limit the functions of any utility to be set up*: the more functions a utility has, the more data it has to process and the more complex, expensive and risky the project becomes.(303)

2. Keep it as simple as possible in legal terms.

The more legally complex an initiative is, the more likely it is to fail. In any case, begin solely with regulated institutions, i.e. ones that are licensed and/or registered. As regards institutions bound by (professional) confidentiality, consider whether they can at least 'extract' information. Finally, it would appear wise to initially limit the scope of any joint utility to be set up to the national boundaries.(304)

3. Ensure appropriate involvement early in the process.

A joint CDD utility is most likely to succeed if senior executives of institutions as well as the relevant public-sector parties are involved at an early stage.

Insights based on the Incident Warning System for Financial Institutions

The Incident Warning System for Financial Institutions demonstrates that it is possible to have information exchange between different (defined) groups of private-sector parties with the aim of more effectively preventing and combating abuse of the financial system - in this case, fraud and deception.

What is important from a privacy perspective is that this exchange of information is proportionate and subsidiary and that the system is also designed with adequate safeguards. Given that criminal data is processed in the External Referral Register (*Extern Verwijzingsregister*, EVR), the Dutch DPA reviewed and issued an authorization for the Incident Warning System for Financial Institutions Protocol.

One of the success factors of the Incident Warning System for Financial Institutions seems to be the decentralization of the information exchange process: the participants remain solely responsible for the data they include about individuals in the Internal Referral Register (*Intern Verwijzingsregister*, IVR) or the External Referral Register (where applicable), and they only exchange information with each other on a need-to-know basis (data minimization). Other relevant factors appear to be:

- Scope of the warning system. In this case, the scope of data processing is national. The international exchange of data, especially outside the EU, greatly complicates the warning system.
- Defined group of participants. Participants in the Incident Warning System for Financial Institutions are all financial institutions licensed under Dutch financial laws and regulations and the five industry associations involved. Given that they are regulated institutions, the group of participants is defined in advance and there is no risk of participants being added beyond what is strictly necessary.
- Clear governance. This is about the roles and responsibilities of participants and industry associations, and the establishment of a guidance committee as well as a process for joining and leaving the Incident Warning System for Financial Institutions. It should also be clear to data subjects (persons whose data is included in the registers) who is responsible for what as regards personal data processing. Data subjects will then know who to go to if they have any questions, requests and complaints.

(303) See also ABS 2018, p. 9.

(304) ABS 2018, p. 8.

- Review system and step-by-step processing structure. This primarily involves inclusion in internal registers, with the possibility for (more) serious cases to be included in external registers. In principle, information is shared on a 'hit/no hit' basis . The sharing of information on further details of an incident is restricted to a defined group of authorized persons (Security Affairs). This is only done after the Security Affairs Department of the questioned institution has conducted its own review regarding the principles of proportionality and subsidiarity.
- Clear rights and obligations for participants. These include requirements with regard to confidentiality, data security, documentation/recording of actions taken and assessments.
- Clear establishment of rights for data subjects. These include the right to be informed and the availability of an objection and dispute procedure. Data subjects also have the right to ongoing access to basic financial products.

4.3 The development and use of digital identities and authentication tools

4.3.1 Digital identities and anti-money laundering policy

A digital identity, or an e-ID, is a digital tool that can be used to verify a person's identity.(305) The amount of information collected in a digital identity depends on the type of digital identity and the system's operation. A digital identity may be limited to primary information, such as given name and surname, place and date of birth, and address information. It could also be in the form of a digital wallet and contain additional personal data and personally identifiable information.(306) This could include information about travel documents, driver's licenses and civil status, as well as education and qualifications, financial data and health.

Digital identities as such are not a new phenomenon and they have been used for some time, especially by government authorities. Many digital identities have so far been developed by and for governments themselves. One example close to home is DigiD, which has been available to Dutch citizens since 2005. They can use it to log in to public-sector parties or organizations bestowed with a public function (e.g. pension funds). Until now, digital identities have mainly been developed for natural persons and to a lesser extent for companies, although there are a few examples of the latter, such as eRecognition ('eHerkenning'). However, introduction of the global Legal Entity Identifier (LEI) in 2012 in response to the financial crisis provided a major push for the development of corporate digital identities.(307) In addition, the EU digital identity, described in Annex B, is expected to become available to companies in 2025.(308)

Identification and verification of customer identity is an important part of customer due diligence, and digital identities and applications are playing an increasing role in this. Establishing business relationships remotely, also known as 'non-face-to-face' or 'remote onboarding', is also becoming increasingly common. The COVID crisis is seen as an important recent driver of this development.(309) Entering into business relationships remotely can include opening bank accounts or taking out insurance through mobile apps. More and more innovative technologies are also being developed to facilitate the establishment of remote business relationships. These could include identifying and verifying the identity of customers via video calls, digital signing of documents and biometric technology. These technologies are also increasingly being developed and offered by commercial operators.

(305) FATF 2020, p. 19.
(306) One example is the digital identity being developed in the European Union: European Commission, 'The European Digital Identity Wallet Architecture and Reference Framework', news release of February 10, 2023.
(307) See Leung et al. 2022 for more information on the origins and operation of the LEI, pp. 16-24.
(308) European Commission, *Digital Identity for all Europeans*, available via this link.
(309) European Banking Authority, *Guidelines for Remote Customer Onboarding*, EBA/GL/2022/15, November 22, 2022, available via this link, p. 4.

The literature highlights the potential benefits of digital identities. They are seen as a tool of choice for financial inclusion, for example, for refugees, the poor or small businesses.(310) The FATF points out that digital ID systems with high assurance levels have the potential to improve the reliability, security, privacy and ease of identification of natural persons across a wide range of services.(311) Specifically, it also underlines the potential for simplifying KYC processes and customer due diligence as regards identifying customers and UBOs and verifying their identity, accelerating turnaround times and thus reducing costs for customers.(312)

It also points to lower risks of errors (due to manual processing of data) and inconsistencies in employee assessments when digital identities are used.(313) As for institutions, these operational efficiencies also free up scarce resources for other purposes. It also draws attention to the benefits obtained in monitoring business relationships when digital identities are kept up to date. One example is transaction monitoring, where changes can be registered immediately.(314)

At the same time, the use of digital identities entails certain risks, particularly in terms of cybersecurity, privacy and fraud.(315) A number of countries are therefore working on assurance frameworks and technical standards for digital identities and solutions. The higher the level of assurance and security of a digital identifier, the greater the degree of confidence that can be placed in it. The FATF as well the EU and national legislatures are in the process of setting conditions for the use of digital identities and applications in laws and regulations. Since May 2020, for example, the Wwft has allowed institutions to use means of electronic identification to establish and verify the identity of customers in customer due diligence. This is conditional on such means meeting a substantial or high assurance level.(316)

It also imposes various requirements on the aforementioned outsourcing, and introductory customer due diligence. However, the responsibility for compliance with the Wwft (and Sw) remains with the gatekeeper.(317) Finally, regulators are paying increasing attention to the use of digital identities and applications.(318)

Annex B details two foreign initiatives relating to digital identities, One is private (Australia Post Digital iD) while the other is a government initiative (the Singaporean Singpass/MyInfo). The deepdive also focused on the impending amendments to the eIDAS Regulation in the European Union. Given that it has direct effect, the Regulation will significantly shape the legislative landscape relating to digital identities and technologies, including existing commercial solutions in the Netherlands. Annex B to this report also sets out details on this.

4.3.2 Insights gained

Developments in digital identities and their use in the EU, which are mainly driven by the European Commission, offer potential for their use in customer due diligence and transaction monitoring.

This is a development separate from (but with considerable similarities to) the development of more private collaboration and information sharing outlined in section 4.2.

(310) Zetzsche et al. 2018, p. 133; Rainey et al. 2019; Leung et al. 2022, pp. 10-11; FATF 2020, p. 14; CGAP 2019.
(311) FATF 2020, p. 13.
(312) Leung et al. 2022, p. 10; FATF 2020, p. 14; DNB 2022, p. 29.
(313) Leung et al. 2022, p. 10.
(314) Leung et al. 2022, p. 11.
(315) FATF 2020, p. 14; Leung et al. 2022, p. 28; ASPI 2022, pp. 8-11.
(316) Section 11(1) first sentence in conjunction with Section 4(1)(h) of the Wwft Implementing Regulation. Section 4(1)(h) of the Wwft Implementing Regulation was added in May 2020, along with the implementation of AMLD5: Implementing Regulation Amending the Fourth Anti-Money Laundering Directive, *Bulletin of Acts and Decress* 2020, 47198.
(317) See Sections 5 and 10 of the Wwft and, by way of illustration, DNB, *Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act*, September 2022, available via this link, pp. 32-34 and 53-54.
(318) See, for example, the EBA Guidelines for Remote Customer Onboarding, EBA/GL/2022/15, November 22, 2022, available via this link.

Where joint utilities devoted to (aspects of) CDD deal with personal data gathered by the private sector based on information they have collected themselves (and verified) as well as from government records, the digital identity also combines personal data, 'proprietary' information and government data. Another similarity is that use of data requires the consent of the data subject.

Initiatives in Australia and Singapore, as well as current possibilities in Europe, show that both private-sector parties and public-sector parties can play an important role in this regard. Besides DigiD and eHerkenning, there are already several private and commercial providers of digital identity, authentication tools (including digital signatures) and digital records management in the Netherlands.

Digital identities currently still seem mainly focused on natural persons; the proposed digital identity with wallet for legal entities seems to be an opportunity to make CDD and transaction monitoring processes more efficient for companies.

The experiences with Singpass/MyInfo show one clear 'lesson learned' for digital identities and their use for CDD and transaction monitoring purposes. To make them a success, we need a supportive government that enables the development of digital identity and its use both technologically and legally. For example, the Singapore government is making all source information on the architecture, operation of the API and conditions for use of Singpass/MyInfo open to all. The Monetary Authority of Singapore, the financial regulator, allows financial institutions to rely on specific identity data from the digital identity without undertaking any additional due diligence.

4.4 Public-private partnerships in the Netherlands

4.4.1 Collaboration between public-sector parties and private-sector parties

As stated in section 4.2, information sharing is seen as an important cornerstone of effective anti-money laundering policy. Public-private partnerships (or PPPs) are mostly forms of collaboration within a specific framework between criminal investigation services, Financial Intelligence Unit (FIU) and the private sector, sometimes supplemented by parties such as ministries, regulators and professional organizations. Potentially, PPPs can help gatekeepers improve their internal processes such as transaction monitoring and enhance the focus of their customer due diligence.(319)

There are more and more PPPs in the EU, although there are differences between the structure, objectives, participants and type of information they exchange.(320) According to the European Commission, PPPs pursuing an anti-money laundering policy are generally set up for two purposes:

- Sharing strategic information between an FIU and gatekeepers on a phenomenon basis (e.g. typologies, trends and risk indicators) or on a specific basis (feedback on FIU reports); and
- Sharing operational information between public-sector parties and gatekeepers about persons or matters that may be of interest to criminal investigations.(321)

The literature calls attention to some (legal) aspects of PPPs. These include privacy and the legal options for information exchange, the impact of information sharing on decisions by the parties in question not to accept certain categories of customers or to terminate the relationship ('de-risking'), and the rights of defendants in criminal proceedings.(322)

(319) European Commission 2022a, p. 20.
(320) European Commission 2022a, p. 2; Vogel 2022, p. 52. To illustrate, on June 22, 2023 it was announced that two pilots were being prepared for more data sharing between banks and public-sector parties in the United Kingdom. It was stated that a form of 'TMNL lite' was to be deployed for one of these pilots: I. Withers and K. Ridley, 'BREAKING: Six British banks to share fincrime information in a 'game changer' plan to crack down on money laundering; Lloyds, NatWest already involved in trials', *AML Intelligence* June 22, 2023.
(321) European Commission 2022a, pp. 2-3. See also Vogel 2022, p. 54.
(322) Vogel 2022, p. 56.

Studies of PPPs in the broader context of subversive crime in the Netherlands also demonstrate the importance of aspects such as the interrelationship between different PPP initiatives, monitoring equality in the relationship between public-sector parties and private-sector parties, and avoiding complexity in the design of collaboration and governance (e.g. sluggish decision-making and trying to reach consensus).[323]

For now PPPs are primarily set up nationally, although the Europol Financial Intelligence Public-Private Partnership project (EFIPPP) is the first and best-known exception to this.[324] A second example is the J5, which in 2022 saw the launch of a public-private partnership between tax investigation services and the biggest banks aimed at tackling tax crime.[325]

In its evaluation of the Netherlands, the FATF praises the public-private partnership initiatives that have been set up.[326] At the same time, it also points to some limitations from a privacy perspective.[327]

As part of this study, four relevant Dutch PPPs with different participants, objectives and scope were explored in more detail. These were Fintell Alliance NL, the Financial Expertise Center (FEC), the Anti-Money Laundering Center (AMLC) and the National Information and Expertise Center (*Landelijk Informatie- en Expertise Centrum*; LIEC) and the Regional Information and Expertise Centers (*Regionale Informatie- en Expertise Centra*; RIECs). The details of these initiatives are set out in Annex B of this report.

4.4.2 Insights gained

The PPPs outlined in the Netherlands each show a different form of public-private partnership:

Fintell Alliance NL is an initiative aimed at exchanging knowledge and strengthening the effectiveness of reporting unusual transactions - based on the existing legal possibilities - between FIU-NL and six banks. Employees of FIU-NL and the participating banks work together in one physical location in this regard. Begun as a pilot, in 2021 it was scaled up to a permanent PPP that was defined in an alliance document. It faces some legal constraints, one of which is that it will only be able to share analyses bilaterally (i.e. between one bank and FIU-NL).[328] However, FIU-NL and the participating banks have found a way to work together within these legal frameworks. Although the criminal investigation services are not directly involved in this PPP, the disclosure of outcomes of Fintell Alliance NL's work to FEC task forces and projects enables them to learn about and make use of this work.[329] The final evaluation of the Serious Crime Taskforce (SCTF) commends Fintell Alliance for the work it supplies to the SCTF.[330]

The FEC PPP collaboration also started out in the form of pilots and it was subsequently enshrined in various covenants. Its main focus is on information sharing between criminal investigation services, FIU-NL and various banks. Information sharing in the SCTF and TFTF task forces takes place within the legal frameworks, although these too are subject to the constraint that banks may only share their analyses bilaterally with FIU-NL. The system of the FEC PPP collaboration is that criminal investigation services, working together with the Public Prosecution Service, share certain intelligence with banks and FIU-NL. Banks can run this information through their systems where they can identify potentially unusual transactions and report them. FIU-NL can declare the reports suspicious and thus make them available to the criminal investigation services. The final evaluation of the SCTF reveals some interesting aspects regarding the collaboration and relationship between public-sector parties and private-sector parties:

(323) Nelen et al. 2023, pp. 190-191.
(324) Europol, *European Financial and Economic Crime Centre - EFECC*, available via this link.
(325) J5 is an abbreviation that stands for Joint Chiefs of Global Tax Enforcement of five international tax investigation services (Australia, Canada, the Netherlands, the United Kingdom and the United States). For the Global Financial Institution Summit in the J5 context, see HM Revenue & Customs and HM Treasury, 'Tax crime chiefs summit commits to international action', press release May 13, 2022.
(326) See FATF 2022b.
(327) Public Prosecution Service 2022, p. 18.
(328) Final Evaluation of the Serious Crime Task Force (SCTF) Pilot, Parliamentary Papers II, 2020/2021, 31 477, no. 60, annex, p. 15.
(329) FATF 2022b, p. 59.
(330) Final Evaluation of the Serious Crime Task Force (SCTF) Pilot, Parliamentary Papers II, 2020/2021, 31 477, no. 60, annex, pp. 15 and 22-23.

- The banks' perception is that the public-sector parties involved are too dominant, and therefore not always transparent.(331) That does not foster trust.
- The banks also feel some discomfort and irritation about their relationship with public-sector parties, which is exemplified by the criminal prosecutions of the former in recent years: "*That is diametrically opposed to trust and collaboration, which I think is the big issue. After all, how are you going to fight crime jointly if at the same time the banks themselves are being fought against?*".(332) This bottleneck, which is perceived by gatekeepers in a broader sense, was discussed in section 3.3.2.
- As regards a possible expansion, reference was made to other gatekeepers that could be relevant to the work and objectives of the SCTF. Examples mentioned are the trust sector, the notarial profession, the legal profession, money transfer companies and payment service providers.(333) However, the argument is that including private-sector parties in the SCTF is too complex: this would require the consent of the FEC Council, an amendment to the covenant and a separate decision under Section 20 of the Police Data Act (*Wet politiegegevens*; Wpg).(334) In future, the inclusion of new private-sector parties in PPPs will be subject to the Data Processing by Partnerships Act (*Wet gegevensverwerking door samenwerkingsverbanden*; WGS).(335)

In 2022, the FEC followed up on the recommendations resulting from the final evaluation. "*'A shared view' about the objective (i.e. common object), direction (common intent) and core values (key principles) of the FEC PPP has been developed.*"(336) The FEC points to the manner in which discussions were held among the parties and notes that "*[t]hat has created further understanding and trust, which is also a solid basis for a sustainable continuation of the FEC PPP.*"(337)

The FATF believes the AMLC has a unique position in the national anti-money laundering landscape.(338) The AMLC has access to a great deal of investigative data if positioned in the FIOD. The AMLC is able to combine this investigative data with publicly available information and, in collaboration with private-sector parties or otherwise, convert it into useful information on money laundering phenomena and typologies for gatekeepers and society at large. Besides the AMLC's added value for public-sector parties in enriching and analyzing information for criminal (preliminary) investigations, it also appears to be able to play an important role in the feedback desired by gatekeepers.

The RIEC-LIEC is primarily a public-public form of collaboration set up with the broader perspective of subversion and organized crime. It also has a strong focus on regional issues. This broader scope and focus sets it apart from the other PPP initiatives mentioned above. Money laundering is a major issue within RIEC-LIEC. Public-private partnerships are not limited to gatekeepers and take place primarily in the form of sharing knowledge and experience through, for example, phenomenon tables and awareness meetings. Public-sector parties and private-sector parties also collaborate on specific projects. However, the fact that not all (private-sector) project partners are signatories to the RIEC covenant has been noted as a complication for information exchange possibilities.(339) Another limitation for information sharing is the legal form of the RIECs. The RIEC is not an independent entity with which information can be shared; at most, the RIEC serves as an intermediary.(340)

PPP initiatives in the Netherlands show that public-private partnerships have different objectives.

(331) Final Evaluation of the Serious Crime Task Force (SCTF) Pilot, Parliamentary Papers II, 2020/2021, 31 477, no. 60, annex, p. 10. According to the literature, this is also a focus area for PPPs in the broader context of organized crime: see, for example, Nelen et al. 2023, on p. 139: "*[...] public-private partnerships lose momentum and dynamism as soon as the public-sector parties exert too much weight in them and take over the helm.*"
(332) Final Evaluation of the Serious Crime Task Force (SCTF) Pilot, Parliamentary Papers II, *2020/2021*, 31 477, no. 60, annex, p. 19.
(333) Final Evaluation of the Serious Crime Task Force (SCTF) Pilot, Parliamentary Papers II, 2020/2021, 31 477, no. 60, annex, p. 37.
(334) Final Evaluation of the Serious Crime Task Force (SCTF) Pilot, Parliamentary Papers II, 2020/2021, 31 477, no. 60, annex, p. 27.
(335) See section 3.2.5.
(336) FEC 2022, p. 18.
(337) FEC 2022, p. 18.
(338) FATF 2022b, p. 60.
(339) Nelen et al. 2023, pp. 80-81.
(340) Arena Consulting & Pro Facto 2022, p. 63.

PPPs can work at the operational level with the goal of bringing together information (networks) to more effectively combat money laundering and terrorist financing. Fintell Alliance and the task forces in the FEC PPP are clear examples of this. PPPs can also work at the phenomenon level, the aim being to share knowledge about phenomena, trends and good practices. The AMLC is a good example of this. What is noticeable is that, at the operational level, the focus of PPPs is primarily on the banks. While understandable given the volume of unusual transaction reports by banks and the focus of government authorities on this gatekeeper group, the positive experiences gained (including reports of better quality and a shorter feedback loop) may be valuable for other gatekeepers as well. Collaboration with other groups of gatekeepers, such as civil-law notaries and real estate agents, is mainly found within/with the AMLC and in broader RIEC-LIEC contexts.

Some lessons can be drawn from the existing PPP initiatives that were explored in this deepdive:

1. Test first, then perpetuate. PPPs typically start with a pilot, after which they are scaled up if successful.
2. Equality. A PPP stands or falls with trust and perceived safety. Important in this regard are equal relationships, commitment, understanding and sufficient transparency between public-sector parties and private-sector parties, to the extent possible within the legal frameworks. Another important aspect is proportional commitment in terms of resources and people. In summary, "*[t]he collaboration [...] should not be a cosy gathering of public-sector parties to which private-sector parties also happen to have been invited.*"(341)
3. Clear governance and clear establishment of objectives, parties, and mutual roles and responsibilities. = Covenants are a common tool in PPPs. The threshold for (private-sector) parties to join a PPP should not be too high.

Care must be taken to ensure that the effectiveness of PPPs is not constrained by a multitude of collaborations or initiatives plus complex governance where the emphasis lies on consultation rather than action.

4.5 Central government steering

4.5.1 Steering of anti-money laundering policy in the Netherlands

Central steering requires having a strategy based on a national risk assessment. A good strategy sets frameworks, provides direction and enables prioritization. In 2019, in response to several money laundering scandals involving European banks, the Ministers of Finance & Justice and Security submitted a joint money laundering action plan to the House of Representatives.(342) In October 2022, this plan led to the bill previously referred to in sections 3.2.1 and 3.2.5.

In September 2022, the Ministers of Finance & Justice and Security sent the Policy Agenda to tackle Money Laundering to the House of Representatives.(343) The policy agenda is based on various studies of Dutch anti-money laundering policy and recommendations resulting from them(344). The ministers have included three themes in the policy agenda based on these studies: 1) strict where necessary, 2) space where possible, and 3) knowledge through measurement. At the highest level, the first two themes relate to the risk-based approach, while theme three is about understanding the effectiveness of anti-money laundering policies. Each theme has sub-themes to which intended operations are linked. In all, the policy agenda lists 31 operations. The Minister of Justice and Security's April 2022 letter to parliament about tackling organized crime shows that preventing and combating money laundering is part of a broader government approach to crime.(345)

(341) Nelen et al. 2023, p. 139.
(342) Parliamentary Papers II, 2018/2019, 31 477, no. 41.
(343) Parliamentary Papers II, 2022/2023, 31 477, no. 80. See Annex 1 for the policy agenda.
(344) Annex 2 to the policy agenda.
(345) Parliamentary Papers II, 2021/2022, 29 911, no. 348, p. 5.

Nevertheless, Chapter 3 shows a clear need for a government with (more) centralized steering, which speaks with a more collective voice, makes clear choices and establishes priorities. Several bottlenecks experienced by gatekeepers and customers can be traced to this point. To explore whether, and if so, where, the steering and prioritization of anti-money laundering policy in the Netherlands could be strengthened, some foreign NRAs were examined more closely. This included looking at recent national strategies and practices in Canada, the United States, the United Kingdom and Italy. For details on this, refer to Annex B.

4.5.2 Insights gained

In practice, NRAs differ in terms of set-up, implementation and reporting. Research also shows that quality is often limited.(346) Making comparisons is therefore challenging. Nevertheless, the comparative analysis reveals some points where foreign NRAs differ from Dutch NRAs and provide inspiration for improving NRAs in the Netherlands. These points relate to the methods of analysis used and to a consideration of sectoral and geographic risks in NRAs or in addition to them.

For Italy, it is noted that preventive anti-money laundering policy is strongly coordinated by the Comitato di Sicurezza Finanziaria (CSF). This committee represents many public-sector parties. Given their joint mission, they are able to share information with each other. In addition to coordinating operations to tackle money laundering and terrorist financing, the CSF is also responsible for drafting the NRA and advising the government by making policy proposals for improving efforts to combat money laundering.

Canada, the United States and the United Kingdom have all recently implemented (government) strategies, which display both similarities and differences between each other. The strategies deployed by Canada and the United States focus specifically on anti-money laundering regulation, while the United Kingdom's strategy includes a holistic, comprehensive approach to tackling economic crime, combating money laundering being one of its priorities.

Whereas Canada and the United States deploy what are really government strategies, the United Kingdom has come up with a joint product of the public and private sectors.

The three strategies are based in part on national risk assessments (NRAs). Common themes include the risk-based approach or strengthening operational effectiveness, and public-private partnerships. All three strategies are layered, setting out top-level priorities and moving down to concrete actions. The United Kingdom's strategy is by far the most specific and detailed in this regard: actions are focused on results (and not solely on effort), are scheduled and include deadlines, and distinguish between responsible and involved parties. A committee made up of representatives from the public and private sectors monitors progress on the strategy.

4.6 From deepdive to possible solutions

The above deepdive reveals a variety of lines of thought and, within them, initiatives in the Netherlands and abroad. There are several ways for gatekeepers to improve the effectiveness and efficiency of compliance with the Wwft and Sanctions Act through collaboration. However, the deepdive also shows that, to achieve this across the board, government plays a crucial role. This involves prioritizing and making choices (central steering), facilitating in terms of information sharing and the use of technological innovations, and engaging in public-private partnerships at the operational level with multiple groups of gatekeepers.

The next chapter discusses possible solutions and connects the findings from the deepdive with the findings set out in Chapters 2 and 3.

(346) Ferwerda and Reuter 2022, p. 19.

Possible solutions

5

5.1 Introduction

This study aims to explore the opportunities and possibilities of improving the efficiency and effectiveness of the anti-money laundering chain and compliance with the Sw through the collaboration of the various groups of gatekeepers or by applying other creative working methods.

Based on the literature study and interviews, the gatekeepers' roles and responsibilities under the Sw and the Wwft were reviewed. Also an inventory was made of the criticisms about the (in)effectiveness of the anti-money laundering policy and, more specifically, of bottlenecks encountered in practice by gatekeepers and customers in the implementation of the Wwft and the Sw, as well as those identified by regulators and the Public Prosecution Service.

What is striking here is that the anti-money laundering policy is a unique and independent policy area within the broader fight against organized crime. It is unique because the government has assigned a very important role to private-sector parties - ranging from large financial institutions to professional service providers like real estate agents and civil-law notaries. It is independent because an entirely separate regulatory framework has been set up for the purpose of preventing money laundering and terrorist financing. Gatekeepers have been designated as an important link in the prevention of money laundering and terrorist financing, and in that regard they have to comply with Wwft requirements. Over the past decade, there has been increasing focus on the fulfillment of the gatekeeper role, particularly prompted by enforcement actions initiated by regulators and the Public Prosecution Service. Combined with the ambiguity that gatekeepers encounter 'at the front end' of the government in the form of - among other things - a lack of clear government steering and prioritization, conflicting laws and regulations, a lack of powers in light of the ever expanding due diligence obligation, uncertainty about the interpretation of the risk-based approach, and limited learning opportunity due to the lack of an effective feedback loop, this has led gatekeepers, out of a sense of tensing up, to do more in recent years than is strictly necessary under the risk-based approach. Customers have also increasingly experienced this in the form of reduced access to the financial system, longer processing times, higher costs and repeated queries. Nonetheless, gatekeepers - with the support of their industry associations and professional organizations - have become increasingly aware of the importance of the gatekeeper role and want to make it more effective and efficient for themselves and for their customers.

Against this background, a deepdive was carried out into the opportunities and alternatives in the Netherlands and abroad that could serve as possible solutions or alternatives for more effective and more efficient compliance by gatekeepers with the Wwft and the Sw. The deepdive shows that the main efforts should concentrate on 1) collaboration and 2) the use of (new) technologies.

Gatekeepers together can already take the necessary specific steps in this regard. Whilst these steps may already help to improve effectiveness and efficiency, this study also shows that in order to become truly more effective in preventing money laundering and terrorist financing and in safeguarding the integrity of the financial system, the government's role is crucial. This mainly means supporting gatekeepers, for example through the removal of (legal) hindrances for gatekeepers and the focus on more systematic collaboration between gatekeepers and public-sector parties, allowing gatekeepers to take on their role in a better way. This is also expected to contribute to the motivation of gatekeepers. A tentative first step has been taken in this regard with the roundtable discussions between DNB and the banking sector, of which the outcomes were documented into the NVB Standards.(347)

(347) The first five standards were published by the Dutch Banking Association in May 2023: NVB, 'Minder klantimpact door NVB Standaarden voor risicogebaseerd witwasonderzoek', press release May 30, 2023. The NVB Standards were created in consultation with regulator De Nederlandsche Bank (DNB) and the Ministry of Finance.

Furthermore, for the government, this means taking the lead through central steering and prioritization of the main orientations , laying an even stronger foundation for a clear and supported policy that enables gatekeepers to combat criminal misuse of the financial system by preventing money laundering and terrorist financing effectively and efficiently. Given the outcomes of Chapters 3 and 4 it appears that an important factor in strengthening the anti-money laundering policy is making a clear choice in balancing the importance of privacy on the one hand, and the prevention of money laundering and terrorist financing (and by extension the fight against crime) on the other.

This chapter offers a number of selected possible solutions that can be realized in both the shorter and the longer term to make compliance with the Wwft and the Sw more effective and efficient and that will contribute to realizing a more effective and efficient anti-money laundering approach. In this respect, the possible solutions are divided into three clusters:

1. Possible solutions for which gatekeepers are primarily responsible.
2. Possible solutions for which gatekeepers and government must join forces.
3. Possible solutions for which the government is in the lead.

5.1.1 Complexity and impact of the possible solutions

For each of the possible solutions, an indication is given of the degree of complexity based on the expected effort involved in developing it. The expected effort is estimated based on factors like new or extended forms of collaboration, technological requirements, or impeding factors that have yet to be removed, such as changes to (conflicting) laws and regulations.

This is shown for each possible solution using the following symbols:

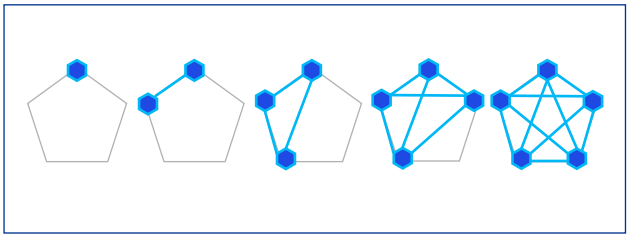


Figure 6: From very little complexity (left) to very high complexity (right)

The expected yield, or the positive impact the possible solution will have on the extent to which the effectiveness of compliance with the Wwft and the Sw increases, is shown for each possible solution using the following symbols:

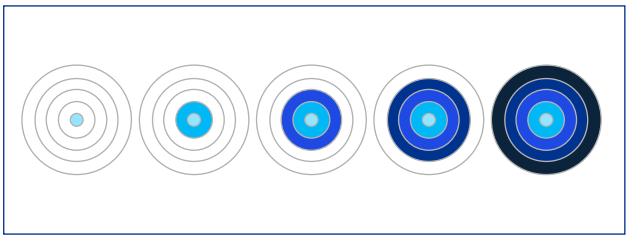


Figure 7: From limited impact (left) to high impact (right)

5.2 Gatekeepers

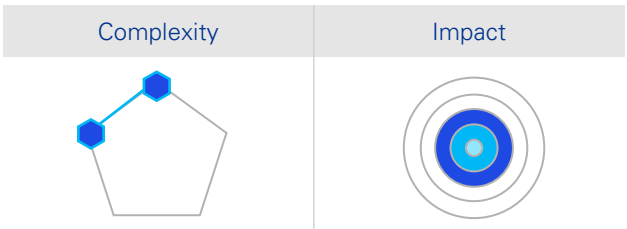
This study reveals a number of opportunities and possibilities for gatekeepers to take steps to improve the efficiency and effectiveness of the anti-money laundering chain and compliance with the Sw through collaboration. It should be noted in this regard that collaboration between gatekeepers is important at all levels. Three specific possibilities are detailed below, but they basically require mutual trust and knowledge exchange between the categories of gatekeepers. Therefore, it is important that gatekeepers (continue to) commit to a (shared) understanding of each other's specific roles and responsibilities in the execution of the joint gatekeeper function, as well as to knowledge about the (nature of the) activities of various gatekeepers. It is also important to liaise on a structural basis to share developments, trends and phenomena. Moreover, gatekeepers should support each other with requests for help, given the nuances in roles, responsibilities and the diverse expertise of the various gatekeepers. In other words, it is important for gatekeepers to look beyond their own sector.

Specifically, there are three solutions for gatekeepers, which are elaborated below:

- Developing a common KYC taxonomy.
- Creating warning systems.
- Developing joint utilities.

5.2.1 KYC taxonomy

A first solution for gatekeepers is to develop a common standard in the field of KYC: the KYC taxonomy.



What is it?

The policies and procedures that gatekeepers have for complying with the Wwft and the Sw are based on various sources, ranging from laws and regulations (European and national), guidelines from national and European regulators and other international organizations, like the FATF, to guidelines and additional requirements or interpretations from industry associations and professional organizations. Given the diversity of the sources, the specific requirements for each gatekeeper may differ; this means that individual gatekeeper policies and procedures will also be different. As a result, in practice, gatekeepers will, for example, use different data points, request different documents from customers, and they will require the provision of more or different forms of evidence or supporting materials to complete the customer due diligence. These differences form an obstacle to an efficient CDD process for both gatekeepers and their customers. A common KYC taxonomy is a joint interpretation of legal requirements, associated data points and underlying documentation.(348)

Why is it important?

A shared KYC taxonomy ensures that gatekeepers collect the same information in a uniform, or harmonized, manner. This offers gatekeepers a stepping stone to more effective and efficient information sharing because they will have the same understanding of the information and thus speak 'the same language'. A shared KYC taxonomy helps in the creation of a warning system and a joint CDD utility (refer to sections 5.2.2 and 5.2.3) and may serve as a relevant information input for a digital identity and 'wallet' (refer to section 5.3.2).

(348) See also NVB 2022a, p. 27.

From the customers' perspective, a shared KYC taxonomy provides clarity and predictability. One can also point to the possibility of reducing the administrative burden and costs.[349] After all, customers will be able to provide the same documentation to different gatekeepers. In this way, customers will not be inconvenienced by repeated requests.

Which specific steps can gatekeepers take?

With respect to the steps to be taken, a distinction can be made between those within the individual category of gatekeepers, and those between different categories of gatekeepers. Although the steps below are presented as sequential steps, in practice several steps may run concurrently.

Specific steps within the individual category of gatekeepers are:

1. Draw up an inventory of the legal requirements (including guidelines plus any expectations of the relevant Wwft regulator), associated data points and source documents by means of a sector-wide request.
2. Identify the legal provisions that are interpreted differently within the sector in terms of data points and/or source documents.
3. Organize roundtable discussions with a representative group of gatekeepers to discuss the different interpretations. This could include assessing which interpretations are 'leading' within the sector and which can therefore be put forward for the common KYC taxonomy.
4. Where agreement cannot be reached and interpretations are directly related to a gatekeeper's own interpretation of the laws and regulations, it is advisable to make enquiries of other gatekeeper sectors about their (common) interpretations.
5. Create a draft shared KYC taxonomy for the sector.

Specific steps between the categories of gatekeepers are:

1. During the process of drawing up the common KYC taxonomy, keep parties within the sector informed, and discuss the differences in interpretations between the sectors.
2. Assess the topics for which a cross-sector common KYC taxonomy is necessary and possible.
3. Organize several roundtable discussions with a representative group of gatekeepers from the different sectors to discuss the different interpretations, and decide what the cross-sector interpretation will be. Where deviations between categories of gatekeepers exist or continue to exist, for example because of differing legal obligations under sectoral laws and regulations or professional regulations, it is recommended that this be stated transparently.
4. Agree the common KYC taxonomy and any sectoral deviations with the Wwft regulators.
5. Establish a final common KYC taxonomy, which clearly indicates any sectoral deviations.
6. Publish the common KYC taxonomy and bring it to the gatekeepers' attention, e.g. by organizing sectoral or cross-sectoral information sessions and by publishing information materials.
7. Evaluate the common KYC taxonomy on a periodic basis, and at the very least when there are relevant changes to laws and regulations.

(349) NVB 2022a, p. 27.

In all the steps to be taken, there is an important coordinating role for professional organizations and industry associations. It is recommended that an independent chair and secretary be appointed to oversee cross-sectoral alignment. They will provide a timeline at the outset as a benchmark, to ensure that cross-sectoral alignment is done efficiently and can be completed in a timely manner.

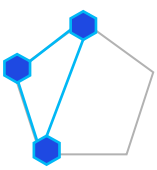
What do gatekeepers need from the government?

Moving toward a common KYC taxonomy does not require a change to laws and regulations. However, it could help gatekeepers if the Wwft regulators offered their support in the creation of a common KYC taxonomy, for example by sharing their interpretations or expectations (e.g. if gatekeepers cannot reach agreement among themselves), by keeping gatekeepers informed of prevailing interpretations elsewhere in Europe based on their international contacts, and by confirming their agreement with the common taxonomy advocated by the gatekeepers.

As for the timing of the alignment with the Wwft regulators, the industry associations and professional organizations could consider seeking alignment at an earlier stage than currently proposed (step 4). As this potentially creates the risk of individual Wwft regulators sharing different interpretations or expectations, we chose to present this in the sequencing at the end of the process when gatekeepers already have the same mutual interpretation in mind.

5.2.2 Warning systems

A second solution for gatekeepers involves the creation of warning systems.

Complexity	Impact
	

What is it?

Each gatekeeper is required under the Wwft to conduct its own customer due diligence. In order to be able to make a good risk assessment, the gatekeeper needs information. This information could, for instance, come from public registers or from customers themselves. Warning systems could further support the activities gatekeepers carry out to protect the integrity of the financial system and to prevent money laundering and terrorist financing. A warning system is a system that contains the data of natural persons and/or legal entities that pose a potential risk to individual gatekeepers or to the integrity of the financial system, for example, in the event of serious suspicions or a conviction of fraud or other criminal behavior. This information is shared and used by gatekeepers (under certain strict conditions).

Why is it important?

The deepdive has already shown that information sharing is seen as one of the cornerstones of an effective anti-money laundering policy. Multiple parties know more and see more than just one: information sharing enables gatekeepers to identify risks better and faster, to limit these risks and to take adequate mitigating measures.

The Protocol on the Incident Warning System for Financial Institutions (*Protocol Incidentenwaarschuwingssysteem Financiële Instellingen*; PIFI) demonstrates that it is possible to share information proactively with each other about customers who are or may be a threat to other gatekeepers or to the integrity of the financial system, whilst respecting the privacy of those involved. Such structured information sharing can actually ensure the adequate protection of personal data because clear mutual agreements are documented in writing.(350) Organizations process personal data in the same way and can also monitor each other in this regard. The PIFI demonstrates that important principles like data quality and data minimization can be met.(351) It also shows that it is important to be mindful of issues like registration criteria, access to the registers, retention periods, deletion of data from the registers and safeguards against the unauthorized use of the data sharing system. Given the threat that fraud as well as money laundering and terrorist financing pose to the integrity of the financial system, it makes sense for other gatekeepers to create a similar system.

The foregoing is particularly relevant since the Cabinet, in its October 2022 Bill on the Money Laundering Action Plan, proposed mandatory data sharing between institutions of the same category for the purpose of carrying out customer due diligence on customers with indications of a higher risk of money laundering or terrorist financing.(352) The Explanatory Memorandum to the bill states that "*[i]n order to reduce the likelihood of a malicious customer gaining access to the financial system through 'shopping' and to avoid the need for each institution to start collecting relevant data from scratch, it is necessary for institutions to exchange information where there are indications that a customer poses a higher risk of money laundering or terrorist financing.*"(353)

Although the bill in its current form raises questions about its mandatory nature, its enforceability, its limitation to high-risk situations (even though 'shopping' is or can be an indicator of such a higher risk) and the restriction on the information exchange between institutions of the same category, this does show that the Cabinet recognizes the importance of information sharing between gatekeepers about risks linked to shared customers.(354) The draft bill also provides a basis for information sharing, by order in council, between different categories of gatekeepers. When customers have to deal with multiple categories of gatekeepers, cross-sectoral information sharing helps create effective information networks to repel criminals. One example applies to real estate transactions, where customers deal with real estate agents, civil-law notaries, banks, mortgage lenders and/or life insurance brokers (or life insurers directly). Large international companies may often have to deal with trust offices, banks, civil-law notaries, tax advisors and accountants (auditors) simply because of the nature of their business. Mandatory data sharing already exists for trust offices under Section 68 Wtt 2018. This due diligence obligation and mutual information sharing between trust offices on proven integrity risks applies to all customer due diligence (and, contrary to the proposal in Section 3b Wwft, not just to higher-risk situations). It also includes the sharing of personal data of a criminal nature.(355)

A broader, proactive warning system for categories of gatekeepers other than banks and insurers, in the same vein as the Incident Warning System for Financial Institutions, could be established under current laws and regulations. It could also possibly be used as a tool for the mandatory information sharing under the future Section 3b Wwft. This would, however, depend on the question of how the data sharing is ultimately given shape in the legislation.

(350) Cf. the PIFI in Annex B.
(351) Required by Article 5 GDPR.
(352) Section 3b of the Bill on the Money Laundering Action Plan.
(353) Parliamentary Papers II, 2022/2023, 36 228, no. 3, p. 5.
(354) See, among other things, *Reactie van NVM, VBO en VastgoedPro op het wetsvoorstel Wet plan van aanpak witwassen*, 2020, available via this link.
(355) Section 68(1) through (3) Wtt 2018.

Which specific steps can gatekeepers take?

One specific step for banks, insurers and trust offices is:

To share the experiences with IFI (banks and insurers) and the mandatory information sharing under Section 68 Wtt 2018 (trust offices) with the other categories of gatekeepers. In doing so, it is recommended that the chosen setup, the necessities from, among other things, a legal and IT perspective (infrastructure including cybersecurity), the required capacity, applicable safeguards and additional relevant privacy considerations be addressed. Furthermore, the costs of the warning system - when it is being set up and on an ongoing basis - can be discussed and the benefits can be explained, possibly using case studies.

Specific steps for the remaining categories of gatekeepers are:

1. To gain knowledge of the experiences that banks, insurers and trust offices have had when using warning systems and mandatory data sharing.
2. To conduct (or commission) a cost-benefit analysis for the creation of a warning system within the sector, as well as a legal analysis where professional confidentiality or other regulations stand in the way of establishing a warning system within the sector.
3. To make an informed decision about the desirability and feasibility of a warning system based on the previous steps.
4. If a decision is made to create a warning system, gatekeepers could draw inspiration from the PIFI and the relevant factors highlighted in Annex B of this report for the further specifics and development.

Specific steps for all gatekeepers are:

1. To monitor developments related to the proposed future Section 3b Wwft as part of the Bill on the Money Laundering Action Plan and to anticipate possible changes to the warning system. In this regard it is important, for both the existing IFI and the warning systems to be created – in view of possible cross-sectoral data sharing – to proceed from the common KYC taxonomy (refer to section 5.2.1).
2. To engage and remain in dialogue with each other during the legislative process and during the development of the systems to ensure that the warning systems that are in place and/or to be developed are both compliant with the legislation and compatible with each other and can be linked to each other for the purpose of possible (future) cross-sectoral data sharing.

What do gatekeepers need from the government?

Some categories of gatekeepers can already start working on the creation of a warning system with the aim of more effectively preventing and combating misuse of the financial system, for example through fraud or deception, without the need for any laws and regulations to change. However, for 'keepers of confidentiality' such as civil-law notaries, sectoral legislation (and/or professional standards) will have to be amended to break the individual confidentiality obligation imposed on these professionals. In the context of the Bill on the Money Laundering Action Plan, the KNB has already expressed support for 'collective notarial confidentiality' and indicated that it had already argued this for some time.[356] For warning systems to function adequately, the insights obtained in section 4.2.3 further revealed that the group of participants must be definable. For real estate agents, this requires government action; see the recommendations in section 5.4.1 on regulation of the real estate profession.

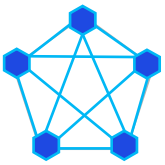
(356) A. Ploumen, KNB: 'Onderlinge gegevensdeling tegen witwassen nodig en gewenst', *MrOnline* November 7, 2022.

Given the possible use of warning systems for the mandatory data sharing included in the Bill on the Money Laundering Action Plan, it is also necessary that there is clarity as soon as possible on what Section 3b Wwft will look like.. This study has previously mentioned the fact that collaboration in the form of networks, partnerships and alliances is increasingly seen as *the* way to act more effectively and efficiently in the fight against money laundering, terrorist financing and underlying crime by criminal organizations. It is therefore advisable to determine, in close consultation with gatekeepers, the situations in which cross-sectoral information sharing is necessary from a Wwft perspective, and at the same time proportionate from a privacy perspective. This is where the so-called 'customer journeys' can play an important role.(357)

When creating a warning system, gatekeepers will need to be mindful of the privacy of natural persons and legal entities that are recorded in the system. The IFI and the underlying protocol meet the requirements of the GDPR. The Dutch Data Protection Authority has indicated that the fight against fraud and the detection of offenders are of great importance, but that criminal data must be updated and shared with great restraint and due care.(358) In the specific steps outlined above, it was stated that gatekeepers could use the PIFI as a starting point for their own sectoral warning system. In all likelihood, this will require a license from the Dutch DPA to process personal data of a criminal nature. In order to ensure that the sectoral warning systems comply with the privacy-by-design principle, it will be necessary for the Dutch DPA to be cooperative so that the right balance can be struck between effectively countering fraud and money laundering on the one hand and protecting personal data on the other.

5.2.3 Joint utilities

A third solution for gatekeepers involves working toward joint utilities.

Complexity	Impact
	

What is it?

This deepdive has already discussed the fact that cooperative efforts , known as 'joint utilities', can focus on different processes like transaction monitoring, sanctions screening (part of) the CDD process.

Initiatives from the Netherlands and abroad show that the development of joint utilities is a relatively young development. The initiatives included in the deepdive (see Annex B) also show that such utilities can be set up in a variety of ways. To summarize, there are currently three common forms:

1. Utility for transaction monitoring. These utilities seem especially relevant to gatekeepers with large transaction flows and long-lasting business relationships, like banks, payment service providers, life insurers, crypto providers and trust offices;
2. Utility for (aspects of) the CDD process in the form of a 'for and by' model, where information is obtained, added and also verified by participating gatekeepers. They are technologically supported by a platform manager. In such instances, the utility functions like a kind of 'repository' ;

(357) For two examples of customer journeys, refer to section 3.3.3.
(358) Dutch Data Protection Authority, *Besluit inzake de vergunningaanvraag voor de verwerking van [PARTIJ] volgens het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021*, August 20, 2021, reference z2021-03355, available via this link.

3. A utility in the form of a service provided by a commercial service provider and to which gatekeepers outsource all or part of their CDD processes. The utility functions could be extended according to the needs of the outsourcing gatekeepers.

Why is it important?

Utilities enable gatekeepers to create networks that allow them to act more effectively and efficiently. In respect of collective transaction monitoring, it has been pointed out that network analyses can see more than an individual bank can, thus allowing a more targeted identification of unusual and suspicious behavior. It is also noted that the transaction monitoring process could become more efficient, that costs could be reduced through the collective development and maintenance of utilities, and that risk management will be improved. The main objective of joint utilities for the CDD process is to make gatekeepers' customer due diligence more efficient through the repeated use of data and the ability to update and optimize this data, known as 'data circularity' and 'data mutualization'. Collaboration between gatekeepers increases the quality and the reliability of data for gatekeepers. For customers, the advantage is that they are not, or are less, inconvenienced by repeated requests and that the customer due diligence runs more efficiently. What is important for the operation of joint utilities for CDD and from the point of view of customer privacy is that collective data processing only takes place with customer consent and that information is only shared between gatekeepers on a need-to-know basis (data minimization). In this way, customers of (participating) gatekeepers are in control of their own data.

Which specific steps can gatekeepers take?

In addition to the steps already taken by banks in the area of collective transaction monitoring and where action on the part of the government is now primarily desired (see more details below under 'What do gatekeepers need from the government?'), working toward a joint utility for different categories of gatekeepers with respect to (aspects of) the CDD process could make a positive contribution to efficient and effective compliance with the Wwft/Sw.

This possible solution is an extension of the possible solutions on the standardization of data points through a common KYC taxonomy and the creation of warning systems (sections 5.2.1 and 5.2.2). It could also converge with the recommendation around the use of digital identities in the context of customer due diligence (section 5.3.2).

A utility for (aspects of) the CDD process is challenging to implement from a practical, legal and technological perspective. Gatekeepers will to some extent be dependent on the government if, in light of privacy protection, the government favors a stronger legal basis for information sharing and collective data processing by gatekeepers and changes to relevant laws and regulations prove necessary as a result. In the meantime, gatekeepers can already take the following steps themselves:

1. Develop a joint action plan for the establishment and operation of a CDD utility (pilot) based on initiatives explored in this study and detailed in Annex B of this report. It is recommended that gatekeepers incorporate, at the very least, the aspects mentioned in section 4.2.3.

   These aspects include, among other things, the group of participants, the type of customers, the desired functions of the utility, the type of information and actualization, the desired technology for the platform, the governance of the utility and aspects like privacy, competition and cybersecurity. The advice is to weigh up, at the outset, whether support will be sought from an independent party who has experience in setting up a complex governance structure, and which has knowledge of and experience in devising and developing a complex technological platform and ensuring compliance with the appropriate privacy guidelines.

   Based on the insights gained, it is also recommended that the initiative starts on a small scale.

This can be done by limiting the group of participants and by limiting the functions of the utility for example, by limiting it to the collection of data and/or the validation of this data. It is also important to keep the set-up and operation of the utility as legally simple as possible; therefore, it is advisable to start the initiative with regulated institutions only, to allow professionals subject to confidentiality only to 'collect' information, and to set it up for national use initially.

2. Despite the recommendation to start small, (regulated) gatekeepers can already assess internally whether there is interest within the sector to participate in the pilot. It should be recognized that creating, and participating in, a joint utility may involve considerable investment in the start-up phase.
3. The insights gained from the deepdive show that the early involvement of relevant public-sector parties is very important. It is therefore important for gatekeepers to consult with, at least, the Wwft regulators and the primarily responsible ministries (the Ministry of Finance and the Ministry of Justice and Security) when developing the proposal and the pilot. Parties can discuss any ambiguities and consider how the government can further support the establishment and operation of a CDD utility (possibly in the form of funding/subsidization and the amendment of laws and regulations).

What do gatekeepers need from the government?

The deepdive into foreign initiatives revealed that these initiatives were all created and/or managed by private-sector parties and that the government only has/had a supporting role.

With regard to collective transaction monitoring by banks, the Bill on the Money Laundering Action Plan provides the legal basis for TMNL. It is important that this legal basis for collective transaction monitoring be in place in the foreseeable future so that the full potential of TMNL can be utilized.

When the bill is considered, it is recommended that collective transaction monitoring be made possible not only for banks, but also for other gatekeepers with large transaction flows and long-lasting business relationships, like payment service providers, life insurers, crypto providers and trust offices.

Initiatives from abroad show (tentatively) that CDD utilities can already be deployed without the need to change laws and regulations, especially since they rely on sharing information about shared customers with the customer's consent. However, given the tension between privacy and the anti-money laundering regulations, it is not inconceivable that governments may want a stronger basis and more safeguards in anti-money laundering regulations for information sharing between, and collective data processing by, gatekeepers. Here, reference can already be made to the fact that, in the negotiations on the AMLR (refer to section 3.2.1) at European level, the Dutch government, together with the governments of Denmark and Germany, is committed to increasing the effectiveness of the gatekeeper role through cooperation and innovation.

The 'Non-paper on enhancing gatekeepers' effectiveness through cooperation and innovation', published in May 2023, recognizes that sharing information about customers or outsourcing tasks can contribute to the fulfillment of the gatekeeper role.(359) In this regard, the governments argue that it is important for anti-money laundering regulations to contain clear rules on information sharing, responsibilities and safeguards. The governments indicate that, from a GDPR perspective, it is important for a common processing ground to be enshrined in the AMLR. In addition, they state that "*[s]ince joint utilities can take on different forms, it is more suitable to leave it to national law to prescribe the specific measures and safeguards that are required for the specific joint utility.*"(360)

(359) Letter from the Minister of Finance on the progress of the Policy Agenda to Tackle Money Laundering: Parliamentary Papers I, 2022/2023, 31 477 and 34 08, D[1] (the letter D only relates to 31 477). The non-paper is included in Annex 6.

(360) Parliamentary Papers I, 2022/2023, 31 477 and 34 08, D1, Annex 6, page 4.

The further elaboration of the requirements of and safeguards for utilities should thus take place at national level, according to the Danish, German and Dutch governments. It was unclear at the time of this study whether these proposals will be reflected in the final text of the Regulation. As noted in section 3.2.1, trialogue negotiations were taking place at the time of this study.

If the European regulations are amended in line with the proposals of the Dutch, Danish and German governments, this would, or could, be a positive step for gatekeepers from the perspective of effective and efficient compliance with the anti-money laundering regulations, as it provides a stronger basis for the collective processing of personal data than if done solely with customer consent. In that case, further choices will have to be made at national level, which the government can already initiate. The following are two things that the government will, in any case, have to arrange:

1. The government will need to clarify, as soon as possible, how the utilities for all or part of the CDD process legally qualify. This is particularly relevant to the joint 'for-and-by' utilities. As regards the introductory customer due diligence, an amendment to the Wtt 2018 will be required for trust offices. Trust offices can only currently use introductory customer due diligence if the introducing institution is also a trust office and belongs to the same group as the trust office.(361) This limits trust offices in participating in joint CDD utilities. It will also be necessary to consider whether real estate agents will be allowed to act as introducing institutions. After all, on this point, the Wwft is more stringent than the current AMLD5.(362)
2. The government will also need to determine the desirability of a licensing regime as soon as possible. In doing so, inspiration may be found in the - so far - only EU Member State with specific anti-money laundering rules on KYC utilities: Latvia.

5.3 Gatekeepers and government

This study also presents a number of other opportunities and possibilities for improving the efficiency and effectiveness of the anti-money laundering chain and compliance with the Sw, whereby gatekeepers and public-sector - respecting their own roles and responsibilities – must join forces.

Specifically, there are two possible solutions: strengthening public-private partnerships and using digital identities in the context of customer due diligence.

5.3.1 Public-private partnerships

A first solution for gatekeepers and government together concerns the continuation and expansion of a structural cooperation between public and private-sector parties.

The formation and continuation of public-private networks in the form of partnerships is crucial to the effectiveness of the anti-money laundering policy. Public-private partnerships (PPPs) within the anti-money laundering policy can take place 1) on a phenomenon basis, through the mutual sharing of knowledge about phenomena, trends and good practices and 2) on an operational level, where the goal is to bring together information on transactions, reports and other intelligence to combat money laundering and terrorist financing more effectively.

(361) Section 21(1) Wtt 2018.
(362) In the Explanatory Memorandum to the Act Implementing the Fourth Anti-Money Laundering Directive (Parliamentary Papers II, 2017/18, 34 808, no. 3, p. 25) it is stated: "*Section 5(1)(a) lacks reference to domicile providers, real estate agents, valuable goods dealers, gambling providers, appraisers and pawnbrokers, among others. This is already the case under the current legislation. The choice not to change this when implementing the Fourth Anti-Money Laundering Directive lies in the fact that the nature of the aforementioned institutions is so different from the nature of other Wwft institutions that it is not obvious for the same level of risk assessment to underlie the customer due diligence of these institutions.*"

In the Netherlands, PPP cooperation takes place both on a phenomenon basis (e.g. AMLC, RIEC-LIEC) and on an operational level (e.g. Fintell Alliance and FEC PPP Serious Crime Task Force (SCTF)).

The insights gained from the deepdive show that creating an equal relationship between the public and private-sector partners is a key consideration in public-private partnerships. Mutual trust, perceived security, commitment, understanding and sufficient transparency form an important basis for effective cooperation. The proportionate deployment of people and resources also plays an important role in this. Furthermore, the deepdive shows that PPP initiatives benefit from transparent (non-complex) governance and a clear recording of the goals, parties, and mutual roles and responsibilities.

The PPP initiatives in the Netherlands that were reviewed in this study show that structural collaboration on operational information (like transactions, reports and other intelligence) in a PPP context is mainly done by banks at the moment. Although there are restrictions on the possibility of targeted information sharing, the experiences in doing so have generally been positive. It is therefore recommended that this form of PPP be continued and expanded to other categories of gatekeepers. Gatekeepers and government should take joint steps in this regard. However, based on the insights gained, it would be necessary to ensure that too many different forms of PPP are not created. It should also be prevented that concrete actions become subordinate to consultation and decision-making. Based on the insights gained, it is recommended to start this new PPP initially through short and concrete pilots, to evaluate them and then move towards a sustainable form of cooperation. Consideration could also be given to allowing categories of gatekeepers other than banks to join existing PPP initiatives, like the SCTF.

While the foregoing recommendation is directed at both gatekeepers and the government, there is still a crucial precondition that has to be realized by the government. To *really* be able to work together effectively and make an impact, it must be made legally possible to share information in a targeted way – between the public-sector partners themselves, between the private-sector partners themselves, and between the public and private-sector partners.(363) While the original aim of the Bill on the Data Processing by Partnerships Act (*Wet gegevensverwerking door samenwerkingsverbanden*; WGS) was to provide a sound basis for the processing of personal data in partnerships, the bill has been amended several times, has been curtailed and still has not been adopted due to privacy considerations.(364) Even traffic light agreements - for example the collaboration between real estate agents, municipalities and the police to combat crime in the rental sector - which were seen as positive by both the private and public sectors, have been terminated due to the lack of a legal basis and restrictions ensuing from privacy legislation.(365) It is time that this legal basis be created.

Specific steps that gatekeepers and government can take within the FEC PPP are:

1. To explore a possible extension to the SCTF in the form of a short pilot with (in any case) trust offices and civil-law notaries. Holland Quaestor and the KNB could enter into discussions with the public-sector participants (the police, the Public Prosecution Service, FIU-NL and FIOD) about the pilot's objectives, methods and governance.
2. Based on the foregoing, the professional organizations can ascertain which organizations from the groups they represent are willing to participate in this pilot, also taking account of the size of the institutions given the expected commitment.

(363) See also the recommendation 'Create a valuable feedback loop' in section 5.4.1.

(364) See section 3.2.5.

(365) Parliamentary Papers II, 2017/2018, 29 911, no. 180.

3. Based on the first two steps, those gatekeepers and public-sector parties that are involved can make further arrangements about the short pilot.
4. Based on, say, two meetings with the pilot group and the relevant public-sector parties, the approach to the cooperation can be honed and the group of organizations involved can be expanded.

A specific step that gatekeepers and the government can take within the RIEC-LIEC is:

To establish systematic, operational cooperation on real estate in the form of (renewed) traffic light agreements between, at the very least, real estate agents, municipalities and the police. For this, it is important for the RIEC-LIEC agreement to provide for the possibility of information exchange between current RIEC-LIEC covenant partners and relevant private-sector parties, like real estate agents. Given the absence of regulation of the real estate profession (see the recommendation in section 5.4.1), it is recommended to limit cooperation to those real estate agents affiliated with industry associations.

5.3.2 Digital identity

A second solution for gatekeepers and government together concerns (working towards) the use of digital identities in the context of customer due diligence.

As indicated in section 4.3, digital identities are not in themselves a new phenomenon and digital authentication tools are playing an increasing role in the identification and verification of customers' identities, for example in the context of 'non-face-to-face' onboarding. The use of digital identities and authentication tools offers both gatekeepers and customers various operational efficiencies in terms of customer due diligence.(366) As regards ensuring privacy, reference can be made to the fact that the use of the data requires the consent of the individual concerned.(367) Also, under the anti-money laundering regulations and eIDAS Regulation, digital authentication tools are subject to assurance requirements.

The insights obtained from the deepdive focus on the one hand on gatekeepers (much is already possible) and on the other hand on government (support and enable).(368)

Gatekeepers

Gatekeepers themselves can already take several preliminary steps regarding the use of digital identities and authentication tools by:

1. Starting to use digital authentication tools (e-ID tools) with eIDAS level 'substantial' or 'high' within the current legal frameworks of the Wwft/Sw. Pending government determination (see recommendation 1 for the government below), professional organizations and industry associations can already support the groups they represent by assessing for the gatekeepers which providers of authentication tools meet the required assurance levels. An external party could prepare the so-called 'vendor selection', based on its knowledge of and experience with the technological capabilities and relevant preconditions, which it will present when this list is prepared.

(366) See section 4.3.1.
(367) What is relevant to the legal validity of the use of consent in accordance with Article 6(1) in conjunction with Article 4(11) GDPR is that, in principle, there should be no negative consequences attached to it. That is to say, the relevant underlying service must also be available to the data subject through other means.
(368) See section 4.3.2.

2. Based on the common KYC taxonomy (refer to section 5.2.1), determining for which data points and source documents it would be desirable to link to digital identities via the 'wallet', and sharing these desires with the government. This should take account of the fact that only those data that come from a reliable and independent source should be included in the wallet.(369)

3. Exploring options for joining, or developing, a trust framework for the purpose of complying with the Wwft/Sw. Trust frameworks regulate the exchange of personal data, for instance in terms of governance, the roles and responsibilities of participating parties, services provided, technical specifications, security requirements (including cybersecurity), privacy and legal aspects. It is recommended that other stakeholders, like trust service providers, software vendors as well as the government, be involved. It is also relevant to consider the customer perspective (natural persons and legal entities); customer journeys can be used to determine where the use of digital identities and items from the wallet would add the most value.

Government

The government has an important role in creating trust in the use of digital tools in the context of the Wwft and the Sw. Two steps can, in any event, be taken for this purpose:

1. In the short term, it is important for the government to support gatekeepers in clarifying which identification tools (e-ID tools) and which providers of these tools meet the assurance level of 'substantial' or 'high'. At the moment, this is left to the individual gatekeepers themselves. For example, the DNB Q&A Electronic means of identification and client identification states the following:"*[i]nstitutions that consider accepting an eID in the context of carrying out the required customer due diligence measures must therefore determine themselves, or through a relevant expert, whether a specific eID tool is a sufficiently reliable means of identification as intended for this purpose.*"(370) Since there is no clear assessment framework for gatekeepers and this creates the necessary ambiguity and involves considerable efforts by gatekeepers, this hampers (especially small) gatekeepers in using such tools. If the government made this information available, gatekeepers could focus on their customer due diligence and setting up a (more) efficient process.

2. In the medium to long term, it is important for the government to work on an early realization of the European digital passport and the attributes for the wallet, taking account of gatekeepers' desires on data points and source documents (refer to step 2 for gatekeepers). It is also important for the government to encourage their use in a Wwft/Sw context, for example by designating European digital passports as an independent and reliable source of certain static customer data and by allowing gatekeepers to rely solely on that information for customer due diligence (i.e. no additional verification/sources needed).(371)

5.4 Government

Achieving a more effective anti-money laundering policy also requires the government - and, where changes to the legal and regulatory framework are required, the legislature - to start taking specific steps. As already noted in the introduction to this chapter, the time seems to have come for the government, more than before, to motivate gatekeepers to perform their role to the best of their ability by providing them with clarity and support 'at the front end'.

(369) DNB 2022, p. 30.
(370) DNB, *Q&A Electronic means of identification and client identification*, available via this link.
(371) See Annex B, section 2.

Going back to the core of the anti-money laundering policy, it is about the government taking a clear governing role through which it provides (high-level) central steering and thereby prioritizes actions on the basis of the NRA.

Recommendations specifically directed at the government and the legislature focus primarily on this supporting role government has with respect to gatekeepers. This includes resolving conflicts or ambiguities in laws and regulations that interfere with effective performance of the gatekeeper function and providing support in the form of guidance and/or feedback. Secondly, the recommendations cover taking ownership and stronger central steering, prioritization and improving the risk orientation. Stronger central steering, an enhanced understanding of the actual risks of money laundering, terrorist financing and the evasion of sanctions, and clear prioritization based on the risks will enable gatekeepers, but also the government itself, to deploy (scarce) resources as effectively and targeted as possible.

5.4.1 Supporting government

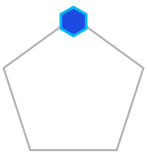
Gatekeepers need to know their customers and the risks they pose and mitigate those risks as much as possible to prevent money laundering and terrorist financing and thereby safeguard the integrity, stability and reputation of the financial system. Despite the fact that combating crime is a core task of the government, the government has assigned an important role to gatekeepers within the anti-money laundering policy. In order to optimally fulfil the gatekeeper role, it is important that gatekeepers are enabled to do so, for example by providing them with an adequate set of powers and the necessary clarity. The bottlenecks identified in Chapter 3 reveal some specific desires for increasing the effectiveness and efficiency of compliance with the Wwft and the Sw. This leads to five recommendations, which are described in more detail below.

The government can already take action on these recommendations, for example by including them in ongoing legislative processes. For the remaining recommendations, it is desirable that the government consults the gatekeepers' industry associations and professional organizations on how and in what time frame they can be followed up on.

1 Work on reliable, public registers and ensure adequate access t for gatekeepers

As a basis for relevant information and data for customer due diligence, it is important that information from public registers are (as) reliable (as possible). To prevent extra work for gatekeepers, they should in principle be able to rely on this data. There are five specific actions in relation to public registers that are required. It should be noted here that for some of the actions the government has already made commitments, but these have still only been implemented in a limited way.

1.a. Retain access to the UBO register for gatekeepers and all institutions that fall within the scope of the RtSw 1977 and grant them access to the closed section of the UBO register as well

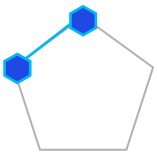
Complexity	Impact
	

The consultation of the Restriction of Access to UBO Registers (Amendment) Act provides for access to the UBO register to gatekeepers and institutions that exclusively fall within the scope of the RtSw 1977 (including non-life insurers). This is a positive first step and gatekeepers therefore hope that the Amendment Act can be passed in the foreseeable future.(372)

(372) See the proposed Section 22a(1) of the Business Register Act 2007 in the consultation of the Restriction of Access to UBO Registers (Amendment) Act. For a further explanation, see also pp. 14-19 of the accompanying draft Explanatory Memorandum. The consultation on the Restriction of Access to UBO Registers (Amendment) Act was launched on May 30, 2023 and is available via this link.

However, what is not yet regulated, is the access to the closed section of the UBO register. However, under the EU AML Package, in particular the proposed Anti-Money Laundering Regulation, the mandatory data for identifying and verifying the identity of UBOs is likely to be significantly extended.(373) This includes data not currently accessible to gatekeepers in the UBO register, like full place and date of birth and residential address.(374) During the completion of this study, the trilogue negotiations on the EU AML Package were in progress, but the Commission, Council and Parliament appeared to be united in wanting to extend identification data for UBOs. This is why gatekeepers should be granted access to the closed section of the UBO register; or the usefulness and necessity of a closed section should be reconsidered.

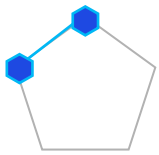
1.b. Provide gatekeepers access to the BRP to perform their customer due diligence

Complexity	Impact
	

Gatekeepers do not have access to the Personal Records Database ('BRP') under the Wwft.(375) Following on from the foregoing, the EU AML Package will in all likelihood also expand the mandatory customer identification and identity verification data. For instance, gatekeepers will be required to identify and verify the nationality (or nationalities) and national identification number of natural persons as part of their customer due diligence.(376)

This expansion could also be accompanied by the power for gatekeepers to be able to verify this information at the source, in order to avoid a further imbalance between duties and powers.(377)

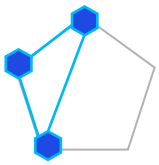
1.c. Take action on ongoing legislative initiatives that could assist gatekeepers in complying with their Wwft obligations more effectively and efficiently

Complexity	Impact
	

A Central Shareholders Register (*centraal aandeelhoudersregister*, CAHR) with up-to-date and verified information on the shareholders of private limited company and unlisted public limited liability companies could make customer due diligence more effective and efficient. Allowing a 'search by name' for persons in the Business Register would also better enable gatekeepers to identify unusual activity, for instance where a natural person appears to be involved in several (seemingly unrelated) businesses. Initiatives to change laws and regulations, or discussions on them, have been going on for a long time in part because of their impact on privacy. It is time to take steps on these dossiers to give gatekeepers the means – while respecting data subjects' privacy through preconditions and safeguards ('privacy-by-design') – to perform their role more effectively and efficiently.

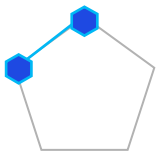
(373) See section 3.2.1.
(374) Article 18(2) in conjunction with Article 44(a) AMLR (proposal). The Anti-Money Laundering Regulation is currently in the trilogue phase between the European Commission, the Council of the European Union and the European Parliament. It is clear from the European Parliament's position that it wants an additional data point for identifying UBOs, namely the Tax Identification Number. In the Netherlands, this is the citizen service number (*burgerservicenummer*, BSN).
(375) There was some talk about opening this up to banks and civil-law notaries for the purpose of conducting customer due diligence under the Wwft, but the Cabinet's pledge to regulate this has not yet been followed up on.
(376) Article 18(1) AMLR (proposal). Article 44(4) AMLR (proposal) states that data for identifying and verifying natural persons must be obtained from an identity document and information from reliable independent sources, or through the use of digital identification tools.
(377) See section 3.3.1.

1.d. Consider further support for gatekeepers by creating registers for which gatekeepers currently often have to use commercial providers

Complexity	Impact
	

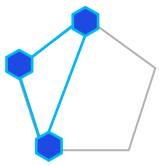
These include, for example, a public register of politically exposed persons (PEP register) that gatekeepers can access as part of their customer due diligence or up-to-date sanctions lists used by institutions in sanctions screening.(378) Currently, gatekeepers often use commercial service providers for this, or they do manual checks against the applicable sanctions lists. By making a complete, up-to-date sanctions list and PEP register available to gatekeepers, the government can support gatekeepers in complying with laws and regulations more efficiently because they can directly rely on the information and also reduce their costs.

1.e. Consider performing sanctions checks against public registers by the government and relax the research effort of companies

Complexity	Impact
	

Every company is supposed to investigate its customers' ownership and control structure to determine whether or not they are under the influence of a sanctioned person. To somewhat relieve companies, including gatekeepers, of this obligation, the Chamber of Commerce (*Kamer van Koophandel*; KVK) could be tasked with conducting sanctions checks on the information recorded in the Business Register and UBO register. When there are actual or suspected sanctions, the Chamber of Commerce should be able to make a note in the register. Although this does not relieve parties of their own obligations - which are broader than just the data contained in the two registers - it may "*contribute to a broader understanding that there are sanctions in place.*"(379) A more robust role for the Chamber of Commerce also fits in with the developments under the EU AML Package. The proposals would require the registrars of UBO registers to verify the accuracy of UBO data. To this end, registrars would, or should, even be empowered to conduct on-site inspection at companies.(380)

2 Create a valuable feedback loop

Complexity	Impact
	

The call for an effective feedback loop from gatekeepers may have existed as long as the reporting obligation itself. Aggregate feedback in the form of typologies and case studies based on reports are already shared.(381) Annual reviews by FIU-NL also provide some insight into the usefulness and value of unusual transaction reports in a general sense. What is currently missing is individual feedback at the level of the reporting organization or transaction to which the report relates. Gatekeepers can learn from this by taking the knowledge back into the organization.

(378) Abroad, PEP registers have in some cases been made available to gatekeepers by governments, for example in Denmark. Gatekeepers may base their due diligence on this: refer to Section 18(7) in conjunction with Section 2(8) of the Hvidvaskloven (the Danish equivalent of the Wwft).
(379) Hoff and Hoff 2023, p. 11.
(380) The European Commission and the European Parliament take the position that registrars should be given this power, while the Council of the European Union does not want to place this obligation (at this stage) on the registrars of UBO registers and wants the power of on-site due inspection to be a Member State option.
(381) For example, via the Knowledge Bank and newsletters from FIU-NL available from the website www.fiu-nederland.nl.

It can also have a positive effect on the willingness to report and the quality of reports.(382) Currently, FIU-NL only provides individual feedback once a report of an unusual transaction is declared suspicious. This is an automated communication with no substantive explanation.(383)

In the Policy Agenda to Tackle Money Laundering, improving the understanding of the use of suspicious transactions and the feedback loop have been identified as a priority. However, the policy agenda does not indicate how improvements to the feedback loop will be implemented.(384) It was also indicated earlier in this study that the Public Prosecution Service is working on this with FIOD, FIU-NL and the police within the Suspicious Transaction (*verdachte transactie*; VT) Working Group and that the banks have recently joined this working group.

Sectoral feedback loop

For the creation of a valuable feedback loop a start can be made by providing sector-wide feedback on outcomes of reports made by that sector over a certain period by FIU-NL, possibly together with criminal investigation services, within the current legal frameworks. For a valuable feedback loop at individual level, FIU-NL and criminal investigation services should be legally enabled to provide feedback to reporting institutions at individual level, without sharing specifics or jeopardizing the ongoing investigation.

Providing sector-specific feedback on reports made over a particular period already gives a sector a greater ability to understand the usefulness and value of reports compared to the aggregate feedback that is currently shared. FIU-NL could provide periodic information to the professional organizations and/or industry associations for this purpose, taking into account any needs about the nature of the information from the various sectors.

Sector-specific feedback could also include investigative intelligence; this could be provided to FIU-NL by criminal investigation services if requested, or criminal investigation services could provide sector-level feedback together with FIU-NL within the possibilities of the legal frameworks.

Individual feedback loop

In developing a feedback loop on individual reports, FIU-NL may be able to learn from experiences abroad. To set up the feedback loop, a standard deadline for feedback on unusual transaction reports based on subjective indicators could be considered. Regardless of whether a report is declared suspicious, a reporting institution will receive feedback with a general reason (on a categorical basis) after a certain period of time of the report being made.(385) One reason may be that a report was qualitatively inadequate; gatekeepers can then address this. If unusual transactions are still declared suspicious within a five-year period, for example through a link to reports made to FIU-NL at a later point in time, a foreign FIU request or new information ensuing from the criminal investigation, the gatekeepers could be informed once again about the report being declared suspicious with an accompanying categorical reason.

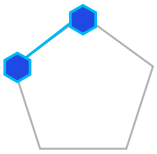
Technology can help to make the individual feedback loop process more efficient. If gatekeepers are put in a position to 'track' the aforementioned feedback moments at an individual level in a system, they can themselves check on the status at any time. This automation might also have a lower impact on FIU-NL in terms of workload.

(382) See section 3.3.2; DNB 2022, p. 6.
(383) FIU-Netherlands, *I have reported an unusual transaction. What happens now?*, available via this link.
(384) Parliamentary Papers II, 2022/2023, 31 477, no. 80. The policy agenda is Annex 1.
(385) Categorical reasons for declaring that there are no suspicions could, for example, be that the report contained too little information (quality indication) or that after an analysis no suspicions could be established. Categorical reasons for declaring that a report is suspicious could, for example, be the reasons that FIU-NL currently includes in a general sense in its annual review. See FIU 2021, p. 9.

Understanding the use of suspicious transactions by criminal investigation services and the Public Prosecution Service

With regard to transactions declared suspicious, it is valuable for gatekeepers to gain (more) insight, into the use of the suspicious transactions they report in the criminal investigation process.(386) Criminal investigation services and the Public Prosecution Service should therefore (be able to) provide feedback at least at an aggregate level, for example, in the form of statistics and by sharing case studies. The Policy Agenda to Tackle Money Laundering includes the compilation and annual publication of relevant statistics as an action point.(387) These include the number of criminal investigations and court decisions (convictions, acquittals).(388) The publication of statistics is a step in the right direction and can contribute to providing the desired insight, especially when the figures are supplemented with an explanation from the criminal investigation service and/or the Public Prosecution Service to place them in the proper context.

3 Regulate the real estate profession and consider introducing a Wwft registration obligation for non-regulated professions and institutions

Complexity	Impact
	

As Chapter 2 showed, the real estate industry is susceptible to money laundering. The fact that the real estate profession in the Netherlands is not regulated makes the industry potentially even more vulnerable: there are no minimum quality requirements, nor is compulsory membership of professional organizations required. This makes it virtually impossible to find out how many real estate agents are actually active in the Netherlands because not all of them are affiliated with one of the three industry associations (NVM, VBO and VastgoedPro). This lack of definition may also have an impact on the allocation of powers.(389) It has therefore been argued previously that the real estate profession should be re-regulated.(390)

Given the importance of the gatekeeper role and in that regard a proper balance between tasks and competences, in conjunction with the possible solution on the development of warning systems (section 5.2.2) and the recommendation to give gatekeepers access to the BRP as mentioned earlier in this section, it does in fact make sense to reintroduce regulation of the real estate profession. In this regard, it is important to include the lessons of the past in regulating the profession; regulation should not exclusively be about title protection and swearing in. Regulation of the real estate profession should be accompanied by ongoing quality and integrity requirements - as currently advocated by industry associations NVM, VBO and VastgoedPro vis-à-vis their members - and a ban on acting as a real estate agent if the person does not meet the legal regulatory requirements.

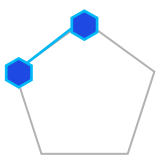
Regulation of the real estate profession could go hand in hand with the introduction of a Wwft registration obligation for unregulated professions and institutions.(391) In addition to the foregoing, the regulator would also benefit from a clearly defined group of regulated institutions, as this would actually allow the regulator to focus the limited resources on carrying out supervision rather than figuring out which parties belong to the regulated population.(392)

Regulation of the real estate profession may also be accompanied by a reconsideration of the current Wwft requirements and practice with regard to customer due diligence performed on the counterparty.

(386) Cf. DNB 2022, p. 6; Netherlands Court of Audit 2022, p. 30.
(387) Letter from the Minister of Finance on the progress of the Policy Agenda to Tackle Money Laundering: Parliamentary Papers I, 2022/2023, 31 477 and 34 08, D[1] (the letter D only relates to 31 477), Annex 2 (Explanation of the status of the Policy Agenda to Tackle Money Laundering).
(388) See the Letter from the Minister of Finance on the progress of the Policy Agenda to Tackle Money Laundering: Parliamentary Papers I, 2022/2023, 31 477 and 34 08, Annex 4.
(389) Hoogenboom 2021, p. 40.
(390) Hoogenboom 2021, p. 171.
(391) Van den Broek 2015, pp. 465-466.
(392) Van den Broek 2015, p. 57.

As indicated in Chapter 3, there is a ban on two-way mediation by real estate agents. As a result, if the buyer and seller both use a real estate agent, they both have to include each other's customers (as counterparties) in their customer due diligence in addition to their own. This means that the due diligence is duplicated. The regulator indicated in the guidelines that real estate agents may outsource the counterparty customer due diligence to each other. However, this still places responsibility for the customer due diligence conducted on the counterparty on the customer's real estate agent. Regulation of the real estate profession with ongoing quality and integrity requirements could be grounds for relying on each other's customer due diligence in this case, with responsibility for the customer due diligence conducted remaining with the real estate agents in respect of their own customers. To do so, however, real estate agents will have to share relevant documentation about each other's customers while ascertaining whether the due diligence conducted on the counterparty (the other real estate agent's customer) meets their own internal requirements and risk classification. If this is not the case, the real estate agent will still have to conduct additional due diligence. Creating a KYC taxonomy, included as a solution in section 5.2.1, could help to harmonize customer due diligence carried out by real estate agents.

4 Protect gatekeepers in case of fear of retaliation for reporting unusual transactions

Complexity	Impact
	

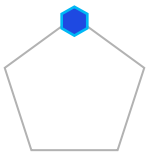
A bottleneck experienced by gatekeepers is the fear of retaliation when reporting unusual transactions to FIU-NL. This is especially true for 'small' gatekeepers, where the company or office name can be the same as the name of the natural person, or because the small number of employees makes it easy to find out who filed the report. However, even employees of large Wwft institutions - like those who have customer contact - are increasingly facing (concrete) threats.

As described in section 3.3.2, some measures have already been taken in recent years and the Minister has announced that she is going to explore various solutions to strengthen the (sense of) security of reporters. It would be appropriate to consider adjusting the manner of reporting in this regard. The AMLD allows accountants, tax advisors, civil-law notaries, attorneys and real estate agents to report through their professional organizations; this Member State option has not been used by the Dutch legislature.(393)

Alternatively, one might consider seeking alignment with schemes like those that apply to witnesses in criminal proceedings, for example. In this case, consideration may be given to making the relevance of the report to the criminal prosecution central: if the report serves primarily as supporting evidence in the criminal trial and, in the opinion of the Public Prosecution Service, the case file contains sufficient other legal evidence to support a finding of guilt, the choice should be made to leave the report out of the case file. If the report is supporting evidence and the Public Prosecution Service is not convinced that the criminal file already contains sufficient legal evidence, the gatekeeper's name should at least be anonymized or pseudonymized. Likewise, the report should be included in the criminal file such that it cannot be traced back to the reporter.

(393) Article 34(1) AMLD5. Article 51 of the draft text (Council version) of the AMLR also includes this possibility.

5 Provide public education about the role and responsibilities of gatekeepers

Complexity	Impact
	

Government support can also take the form of raising awareness. As described in Chapter 2, parties have been designated as gatekeepers for different reasons, and there are differences in emphasis in their roles and responsibilities. To the outside world it may, therefore, be unclear what the gatekeeper role entails, what gatekeepers are supposed to do and what that means in practice for customers. To enable gatekeepers to use their limited resources to fulfill their gatekeeper role, the government should provide more public education.

The Policy Agenda to Tackle Money Laundering, which includes improving the provision of information to customers about the purpose of the Wwft and the information required by institutions for customer due diligence as an action point, is a first step in the right direction.(394) However, the action point elaborates the safeguarding of the payment system and thus the provision of information is limited to the banking sector.

It is recommended that the government seeks to arrive at a broader solution for all categories of gatekeepers. This could include providing a (digital) place where customers can find information on the roles and obligations of gatekeepers in complying with the Wwft and the Sw. The information, however, should go beyond pulling together and listing the applicable laws and regulations and the contact information of relevant public and private-sector parties. The government could also launch a campaign to introduce society at large to the anti-money laundering policy along with gatekeeper roles and responsibilities. Finally, the government could consider setting up a questions and/or complaints office so that gatekeepers can refer customers to the government when they have questions from or a dispute with customers.

5.4.2 Central steering

The anti-money laundering policy in the Netherlands is characterized by a high degree of fragmentation. It is a stand-alone policy, but falls within the broader approach to organized crime. This means that many different public-sector parties are involved, ranging from ministries, regulators, municipalities, FIU, government services and implementing organizations, and criminal investigation services to the Public Prosecution Service. As indicated in section 3.3.2, all of these parties have their own task in combating subversive and/or financial and economic crime and have their own interests to promote. The picture emerges from the interviews that there is a lot of trying to reach consensus between these public-sector parties.(395) This has a negative impact on gatekeepers.

A lack of central steering, including clear prioritization and a balancing of interests, can result in the government not making clear choices, which leads to drifting and getting bogged down in general commitments rather than taking concrete action.(396) As a result, little progress is made in legislative processes, among other things. This is already the case for several legislative processes and projects that affect the preventive anti-money laundering policy. Examples include the legislative processes around the Data Processing by Partnerships Act (WGS) and the Central Shareholders Register (CAHR). Given the tension in the Bill on the Money Laundering Action Plan between effectively combating money laundering and terrorist financing on the one hand and protecting privacy on the other, there is a high risk of a laborious, lengthy legislative process here, too.

(394) Letter from the Minister of Finance on the progress of the Policy Agenda to Tackle Money Laundering: Parliamentary Papers I, 2022/2023, 31 477 and 34 08, D[1] (the letter D only relates to 31 477), Annex 2 (Explanation of the status of the Policy Agenda to Tackle Money Laundering).

(395) See section 3.3.2.

(396) Cf. Nelen et al. 2023, pp. 190-191.

Moreover, it is extremely uncertain whether the bill sent to the House of Representatives in October 2022 will actually be passed in its proposed form. Furthermore, the Policy Agenda to Tackle Money Laundering contains numerous commitments to certain efforts without any concrete results. This can be seen in the way it is formulated: 'examine', 'strengthen', 'explore', 'commit to', 'promote', 'discussions with' are some examples. On top of that, the May 2023 progress report states that some crucial efforts related to cooperation are being postponed due to privacy concerns.(397)

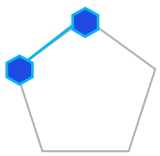
4. Behouden effectieve gegevensdeling en samenwerking	• Bestendigen en doorontwikkelen van samenwerking en gegevensdeling in de aanpak van witwassen, waarbij ook partijen buiten de financiële sector worden betrokken	• Uitgesteld. Naar aanleiding van de zorgen op het gebied van privacy, zie bijvoorbeeld de Wet gegevensverwerking samenwerkingsverbanden (WGS) en het Wetsvoorstel Plan van aanpak witwassen, is het op dit moment niet opportuun om het bestaande stelsel verder uit te werken.
	• Onderzoeken verdere mogelijkheden om huidige samenwerking te verbeteren	• Uitgesteld. Gesprekken met de relevante belanghebbenden zullen wel worden afgerond.
	• Introductie maatregelen uit het wetsvoorstel plan van aanpak witwassen met verbeteringen op het gebied van gegevensdeling	• Loopt. Het wetsvoorstel plan van aanpak witwassen is in oktober 2022 naar de Tweede Kamer verzonden.

Source: Status of Policy Agenda to Tackle Money Laundering - Annex 1 to the progress letter, p. 4.

With an unambiguous government vision in which the various interests of the relevant government parties have been considered in advance and choices have been made, such 'paralysis' can be avoided and action can be taken. This also gives direction and clarity to gatekeepers as to where they should focus their efforts under the risk-based approach and where, in the government's words, 'less can be done'.(398) Gatekeepers then do not suffer, or suffer less, from the paralyzing effects and ambiguities that a lack of unambiguous steering and balancing of interests brings. Clarity contributes to gatekeepers' motivation who can get to work in a(n) (even more) focused manner with the directions provided

Specifically, the foregoing leads to the following recommendations:

1 Appoint a national coordinator on behalf of the government to take the lead in the national anti-money laundering approach

Complexity	Impact
	

Ideally, the coordinator acts on the overall AML approach and connects the public-sector parties and their interests involved. He acts as the driver of an effective and efficient anti-money laundering policy, and is the face or figurehead of this national approach on behalf of the government towards the private sector. In this regard, the coordinator will be made responsible for the following:

(397) Letter from the Minister of Finance on the progress of the Policy Agenda to Tackle Money Laundering: Parliamentary Papers I, 2022/2023, 31 477 and 34 08, D[1] (the letter D only relates to 31 477). The letter has 6 annexes.

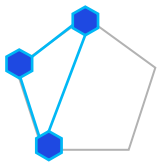
(398) Parliamentary Papers II, 2022/2023, 31 477, no. 80. The policy agenda is Annex 1.

- Ensuring representation of the various (government)interests that affect the fight against money laundering and terrorist financing. This means that the coordinator brings together various government parties at (inter)ministerial level, as well as regulators (Wwft, privacy, competition) and other government services, leading to clear choices being made. Where different interests affect each other and a legal basis needs to be sought, the coordinator should advise the legislature on the (desired) balancing of interests.
- Perpetuating the national anti-money laundering approach in a strategy based on the actual risks to the Netherlands (see also the recommendation 'Strengthen, deepen and expand the national risk assessment') in which choices are made regarding the priorities in the fight against money laundering and terrorist financing (see also the recommendation 'Prioritize and establish a risk appetite for the Netherlands').
- , Stimulating a long-term, systematic cooperation within the national anti-money laundering policy and aligning the various public-private partnership initiatives.
- Ensuring that the national anti-money laundering approach is aligned with other national programs and policy areas, like the broader national approach to subversive (drug) crime and (modernization of) the sanctions system.
- Monitoring the national anti-money laundering approach and advising the government when changes to the approach are necessary to achieve a more effective anti-money laundering policy while respecting associated interests.
- Functioning as the primary point of contact for the private sector, including gatekeepers.

The role can be filled by a natural person, like Stef Blok did (temporarily) as National Coordinator for Sanctions Compliance and Enforcement, or by an organization. In the United Kingdom, for example, the National Economic Crime Centre (NECC) has been designated as the 'system leader' in combating economic crime, money laundering, terrorist financing and proliferation financing.(399)

Where the gatekeeper role and compliance with the Sw and underlying regulations affect each other, cooperation with the national coordinator, or coordinating authority, for sanctions compliance would be logical.(400)

2 Strengthen, deepen and expand the national risk assessment

Complexity	Impact
	

National Risk Assessments (NRAs) are the foundation of a national anti-money laundering strategy and the risk-based approach in the anti-money laundering policy. This study has revealed a need among gatekeepers to gain a better understanding of the actual biggest threats to the integrity of the financial sector.(401)

Better use and deepening of the NRA has already been included by the government as one of the priorities in the Policy Agenda to Tackle Money Laundering.(402) A major focus for improving and deepening the money laundering NRA will be the use of various data sources. Currently, the NRA relies (almost) entirely on expert opinions.(403) However, the literature argues that NRAs ought to consist of multiple sources of information to be credible.(404)

(399) See Annex B, section 4.4.
(400) National Coordinator for Sanctions Compliance and Enforcement 2022.
(401) See section 3.3.2.
(402) Parliamentary Papers II, 2022/2023, 31 477, no. 80. The policy agenda is Annex 1.
(403) WODC 2020, pp. 21-33.
(404) Ferwerda and Reuter 2022, p. 26.

The Policy Agenda to Tackle Money Laundering includes the compilation and annual publication of relevant statistics as an action point.[405] These include, for example, supervisory statistics (number of investigations, number of violations detected, number of enforcement actions) or the number of criminal investigations and court decisions (convictions, acquittals).[406] Keeping statistics is a step in the right direction and can eventually contribute to strengthening the NRA by making it more evidence-based. This requires not only the commitment and efforts of the government (regulation/supervision, FIU, criminal investigation), but gatekeepers will also need to update and share relevant data to benefit the NRA.

Based on an analysis of several NRAs in the deepdive, several other points emerge that could contribute to a meaningful strengthening and deepening of the NRA and give gatekeepers more specific guidance than they currently have. The following suggestions ensue from the insights gained:

1. Consider approaching the NRA from the perspective of the underlying crime, the predicate offenses, rather than the money laundering methods.
2. Consider focusing the NRA on inherent risks.
3. Broaden the NRA by adding geographic risks. This could include listing the economic sectors and financial products most important to the Netherlands and, looking at the nature and extent of trade relationships, transactions with high-risk countries, as well as the risks posed by neighboring countries or countries within the Kingdom of the Netherlands.
4. Deepen the NRA by addressing regional differences within the Netherlands ('regional risk assessments'). The underlying crime and associated money laundering risks may differ between regions. Consider, for example, regions with airports, ports, border areas, urban areas or rural areas.
5. Deepen the NRA by complementing it with sectoral risk assessments that translate and further elaborate the NRA for each gatekeeper category. This provides more specific guidance to the various gatekeepers, which they in turn can incorporate into their own risk assessments.

3 Prioritize and establish a risk appetite for the Netherlands

As the foundation of the risk-based approach, the NRA ideally is the starting point for the national anti-money laundering approach. To be able to exercise central steering (see recommendation 'Appoint a national coordinator on behalf of the government to take the lead in the national anti-money laundering approach'), a strategy and a policy based on it are important. A good strategy establishes a framework, provides direction and enables prioritization. Priorities help to bring focus to the risk-based approach and thus to the deployment of (limited) resources.

It is unrealistic to state that money laundering can be completely prevented with an effective application of the anti-money laundering policy.. Nor is it realistic to expect gatekeepers to guard their gates such that no criminal proceeds enter the financial system at all.

(405) Letter from the Minister of Finance on the progress of the Policy Agenda to Tackle Money Laundering: Parliamentary Papers I, 2022/2023, 31 477 and 34 08, D[1] (the letter D only relates to 31 477), Annex 2 (Explanation of the status of the Policy Agenda to Tackle Money Laundering).

(406) See the Letter from the Minister of Finance on the progress of the Policy Agenda to Tackle Money Laundering: Parliamentary Papers I, 2022/2023, 31 477 and 34 08, Annex 4.

With prioritization in a national anti-money laundering strategy, gatekeeper efforts can focus on the most important national priorities. As not everything can be or remain a priority, this obviously also means that efforts will be less in other areas. It is therefore recommended that the Dutch government, with the NRA and when setting its priorities, also establishes a national risk appetite that, together with the stated priorities, can serve as a bandwidth for the application of the risk-based approach of the anti-money laundering policy, and thus for gatekeepers in the fulfillment their role.

In the Netherlands, the government has already taken positive steps in recent years, including the 2019 Money Laundering Action Plan and the 2022 Policy Agenda to Tackle Money Laundering. However, the insights gained from the deepdive show that further steps need to be taken in the coming years to become even more effective. Thus, ideally, the NRA should not be part of but the starting point for the development of a national anti-money laundering strategy. And within that strategy, clear priorities will need to be set that are specific enough to guide the (expected) efforts of gatekeepers. The recent Economic Crime Plan 2 from the United Kingdom can serve as an example for the Dutch government in this regard: a clear commitment from the private sector in the creation of the strategy and clear priorities with specific elaboration, coupled with clear timelines and continuous progress monitoring.

5.5 From solutions to action

Based on the study conducted, the preceding sections have suggested some possible solutions that could help to improve the efficiency and effectiveness of the anti-money laundering chain and compliance with the Sw, and by extension the effectiveness of the anti-money laundering system in the Netherlands. In this regard a distinction was made between the expected complexity and the impact of the possible solutions. Table 1 lists the possible solutions.

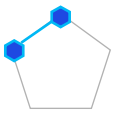
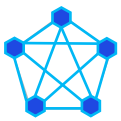
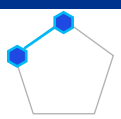
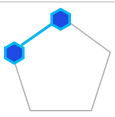
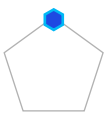
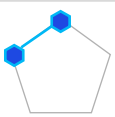
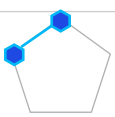
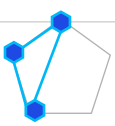
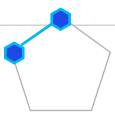
Possible solution	Complexity	Impact
Gatekeepers		
KYC taxonomy		
Warning systems		
Joint utilities		
Gatekeepers and government		
Public-private partnerships		
Digital identity		
Government		
A supporting government		
Public registers • Access to the (closed section) of the UBO register		
• Access to the BRP		
• Ongoing initiatives (CAHR, search function for persons in the Business Register)		
• Public PEP register and sanctions lists		
• Sanctions checks carried out by the government		

Table 1: Complexity and impact of proposed possible solutions (continued on the next page)

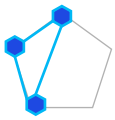
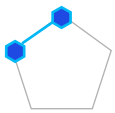
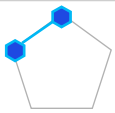
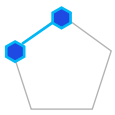
Possible solution	Complexity	Impact
Government		
A supporting government		
Creation of a valuable feedback loop		
Regulation of the real estate profession and Wwft registration obligation		
Protection for gatekeepers where they fear retaliation		
Raising public awareness of gatekeepers' role and responsibilities		
Central steering		
National coordinator		
National risk assessment		
Prioritization and establishing the *risk appetite*		

Table 1: Complexity and impact of proposed possible solutions (continued)

The extent to which the solutions will be realized and their full potential will be utilized will depend on the efforts and commitment of gatekeepers and government. For gatekeepers, it is essential that they (dare to) take the concrete steps within the possibilities available to them . It is important for the government to enable gatekeepers to do so. This involves concerns providing gatekeepers with powers as well as the removal of (legal) ambiguities or conflicts. In view of the expected impact, working towards strong central steering is of fundamental importance. Central steering requires a clear national anti-money laundering approach laid out in a strategy that is based on the actual risks to the Netherlands, and in which clear choices are made on the priorities in combating money laundering and terrorist financing.

Many solutions are affected by the current debate about privacy. Therefore, the highest priority must be given to balancing the importance of privacy on the one hand, and the prevention of money laundering and terrorist financing (and, by extension, the fight against crime) on the other. The current situation in which the two interests keep clashing in different areas - including access to the Personal Records Database (BRP) and the UBO register, the possibility of collective transaction monitoring, the ability or need for gatekeepers to share relevant information about (common) customers, the feedback loop and targeted information sharing between public-private sector parties and between public-sector parties themselves - is not sustainable. The government will have to accept that assigning greater importance to one interest will impose a constraint on the other. As long as that choice is not made, no or only limited steps can be taken in fighting crime.

In short, it is time to turn good intentions into concrete actions. This study shows that this can mainly be done by focusing on collaboration and the use of technology. Gatekeepers cannot do this alone. The government cannot do this alone. They can only do this together. Based on trust.

Annexes

Bibliography

A

A. Bibliography

1. Books and articles/journal publications

Alldridge 2016
P. Alldridge, *What Went Wrong With Money Laundering Law?*, Palgrave Pivot: London, 2016

Amicelle 2017
A. Amicelle, 'Policing through misunderstanding: insights from the configuration of financial policing', *Crime Law Soc Change* 2018, vol. 69, pp. 207-226

Berkvens 2011
J.M.A. Berkvens, 'Het nieuwe Incidentenwaarschuwingssysteem financiële instellingen in het perspectief van de bestaande jurisprudentie inzake inzage en correctie', *Tijdschrift voor Financieel Recht* 2011, no. 7/8, pp. 205-214

Bökkerink and Ligthart 2014
M.J. Bökkerink and M.C. Ligthart, 'De Wwft en de sanctiewet 1977 – overeenkomsten en verschillen', *Tijdschrift voor Compliance* 2014, no. 4, pp. 212-218

Bökkerink 2022
M. Bökkerink, 'De FATF evaluatie van Nederland: een goed resultaat, maar er moet nog wel iets gedaan worden', in: *Tijdschrift voor Sanctierecht en Onderneming* 2022, no. 6, pp. 169-175

Daalderop 2019
A. Daalderop, 'Straf- en bestuursrechtelijke aansprakelijkheid van poortwachters', *Tijdschrift voor Compliance* 2019, no. 1, pp. 45-51

De Vries and Mourcous 2019
E. de Vries and L. Mourcous, 'Privacyrechtelijke aspecten voor het gebruik van een zwarte lijst', *Privacy & Informatie* 2019, aflevering 6, pp. 244-251

Diepenmaat 2021
F. Diepenmaat, '(The Fight Against) Money Laundering: It's All About Networks', in: O.M. Granados and J.R. Nicolás-Carlock (eds), *Corruption Networks. Concepts and Applications*, Springer International Publishing: Cham, 2021, pp. 115-130

Ferwerda and Reuter 2022
J. Ferwerda and P. Reuter, *National Assessments of Money Laundering Risks: Learning from Eight Advanced Countries' NRAs*, World Bank Publications: Washington, 2022

Gilmour and Hicks 2023
N. Gilmour and T. Hicks, *The war on dirty money*, Bristol University Press: Bristol, 2023

Groen and Van den Broek 2023
L.G. Groen and M. van den Broek, 'Ontwikkelingen in het Europese anti-witwasbeleid: het EU Single Rulebook', *Tijdschrift voor Sanctierecht & Onderneming* 2023, no. 1, pp. 13-20

Hoff and Hoff 2023
R.J. Hoff and J.F. Hoff, 'Sancties in ontwikkeling en modernisering Sanctiewet', *Tijdschrift voor Sanctierecht & Onderneming* 2023, no. 1, pp. 3-12

Ipenburg 2023
D. Ipenburg, 'Tussen plan en aanpak. Over het wetsvoorstel Wet plan van aanpak witwassen', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2023, no. 1, pp. 25-31

Kodrzycki and Geertsma 2019
T.J. Kodrzycki and J.G. Geertsma, 'Sanctieregelgeving en Wwft: same same, but different!', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2019, no. 4, pp. 230-237

Lagerwaard 2022
P. Lagerwaard, 'Financiële surveillance en de rol van de Financial Intelligence Unit (FIU) in Nederland', *Beleid en Maatschappij* 2022, vol. 49, no. 2, pp. 128-153

Levi, Reuter and Halliday 2017
M. Levi, P. Reuter and T. Halliday, 'Can the AML system be evaluated without better data?', *Crime Law Soc Change* 2017, no. 69, pp. 307-328

Nelen et al. 2023
H. Nelen, K. van Wingerde, L. Bisschop & R. Moerland, *Koers bepalen. Over de lessen van de versterking aanpak georganiseerde drugscriminaliteit,* Boomcriminologie: The Hague, 2023

Nuijten 2023
S.M.C. Nuijten, 'Van poortwachters en witwassers: Ontwikkelingen in het toezicht op de Wwft', *Tijdschrift voor Financieel Recht* 2023, no. 4, pp. 141-148

A. Bibliography

1. Books and articles/journal publications

Pol 2018
R. Pol, 'Uncomfortable truths? ML=BS and AML=BS^2', *Journal of Money Laundering Control*, vol. 25, no. 2, pp. 294-307

Rainey et al. 2019
D. Rainey, S. Cooper, D. Rawlins, K. Yasuda, Tey Al-Rjula & Manreet Nijjar, 'Digital Identity for Refugees and Disenfranchised Populations The 'Invisibles' and Standards for Sovereign Identity', *International Journal of Online Dispute Resolution* 2019, vol 6, issue 1, pp. 20-56

Rakké and Huisman 2020
J.T. Rakké and W. Huisman, 'Motieven voor naleving van de wettelijke anti-witwasmeldplicht', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2023, vol. 1, pp. 5-11

Reuter 2013
P. Reuter, 'Are estimates of the volume of money laundering either feasible or useful', in: B. Unger and D. Van der Linde (eds), *Research handbook on money laundering*, Edward Elgar Publishing Ltd: Cheltenham, 2013, pp. 224-231

Riekerk 2016
C. Riekerk, 'Integere normen voor trustkantoren', in: *Tijdschrift voor Financieel recht* 2016, no. 11, pp. 433-437

Snijder-Kuipers 2020
B. Snijder-Kuipers, 'Poortwachtersfunctie van de notaris en witwassen', *Tijdschrift voor Compliance* 2020, no. 1, pp. 35-41

Unger and Van Waarden 2013
B. Unger and F. van Waarden, 'How to dodge drowning in data? Rule- and risk-based anti-money laundering policies compared', in: B. Unger and D. Van der Linde (eds), *Research handbook on money laundering*, Edward Elgar Publishing Ltd: Cheltenham, 2013, pp. 399-425

Van den Broek 2015
M. van den Broek, *Preventing money laundering: A legal study on the effectiveness of supervision in the European Union*, Eleven International Publishing: The Hague, 2015

Van den Herik 2022
L. van den Herik, 'De toekomst van VN-sancties', *Ars Aequi* February 2022, pp. 111-117

Verhage 2017
A. Verhage, 'Great expectations but little evidence: policing money laundering', *International Journal of Sociology and Social Policy* 2017, vol. 37, no. 7/8, pp. 477-490

Yeoh 2020
P. Yeoh, 'Banks' vulnerabilities to money laundering activities', *Journal of Money Laundering Control* 2020, vol. 23, no. 1, pp. 122-135

Zavoli and King 2021
I. Zavoli and C. King, 'The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis', *Modern Law Review* 2021, vol. 84, no. 4, pp. 740-771

Zetzsche et al. 2018
D. Zetzsche, D.W. Arner and R. Buckley, 'Digital ID and AML/CDD/KYC utilities for financial inclusion, integrity and competition', *Capco Journal* 2018, vol. 47, pp. 133-143

Zwinkels 2020
J.A. Zwinkels, 'Bestraffing van de compliance bij non-compliance trustkantoor – een reëel risico', *Tijdschrift voor Sanctierecht en Onderneming* 2020, no. 2, pp. 60-73

A. Bibliography

2. Reports

ABS 2018
Association of Banks in Singapore, *Industry Banking KC Utility Project After-Action Report – Knowledge sharing*, November 15, 2018

Algemene Rekenkamer (Netherlands Court of Audit) 2022
Algemene Rekenkamer (Netherlands Court of Audit), *Bestrijden witwassen deel 3: stand van zaken 2021*, June 2022

Arena Consulting & Pro Facto 2022
Arena Consulting & Pro Facto, *Monitor bestuurlijke aanpak van georganiseerde criminaliteit*, November 28, 2022

ASPI 2018
Australian Strategic Policy Institute, *Preventing another Australia Card fail: Unlocking the potential of digital identity*, October 16, 2018

ASPI 2022
Australia Strategic Policy Institute, *The future of digital identity in Australia*, Policy Brief Report No. 66/2022, November 17, 2022

Australia Post 2021
Australia Post, *Annual Report 2021,* 2021

Autoriteit Persoonsgegevens (Dutch Data Protection Authority) 2019
Autoriteit Persoonsgegevens, *Aanvullend advies wetsvoorstel gegevensverwerking samenwerkingsverbanden*, April 19, 2019

Autoriteit Persoonsgegevens 2019a
Autoriteit Persoonsgegevens, *Advies over het concept voor het Implementatiebesluit registratie uiteindelijk belanghebbenden van vennootschappen en andere juridische entiteiten*, July 18, 2019

Autoriteit Persoonsgegevens 2019b
Autoriteit Persoonsgegevens, *Advies inzake toegang tot gegevens voor poortwachters bij het voorkomen van witwassen*, December 16, 2019

Autoriteit Persoonsgegevens 2019c
Autoriteit Persoonsgegevens, *Wetgevingsadvies wetsvoorstel gegevensverwerking door samenwerkingsverbanden*, January 4, 2019

Autoriteit Persoonsgegevens 2023
Autoriteit Persoonsgegevens, *Schriftelijke inbreng Autoriteit Persoonsgegevens Rondetafelgesprek Wetsvoorstel Plan van Aanpak Witwassen,* January 24, 2023

BIS 2023
Bank for International Settlements Innovation Hub, *Project Aurora: The power of data, technology and collaboration to combat money laundering across institutions and borders*, May 2023

Bureau Broekhuizen 2022
Bureau Broekhuizen, *De poortwachtersfunctie van Amsterdamse makelaars*, January 2022

CGAP 2019
Consultative Group to Assist the Poor, *Beyond KYC Utilities: Collaborative Customer Due Diligence for Financial Inclusion*, CGAP Working Paper, August 2019

College van toezicht op de bedrijfsrevisoren (Belgian Audit Oversight Board) 2023
College van toezicht op de bedrijfsrevisoren, *Sectorale WG/FT risicoanalyse 2022*, February 22, 2023

DNB (The Dutch Central Bank) 2017
DNB, *Good Practice: Integrity Risk Appetite*, September 2017

DNB 2019
DNB, *Fiscale integriteitsrisico's voor trustkantoren*, April 2019

DNB 2019a
DNB, *General principles for the use of Artificial Intelligence in the financial sector*, July 2019

DNB 2022
De Nederlandsche Bank, *Van herstel naar balans*, September 2022

EBA 2020
European Banking Association, *Report on big data and advanced analytics,* January 2020

A. Bibliography

2. Reports

EBA 2022
EBA, *Opinion and Report on de-risking and its impact on access to financial services*, EBA/Op/2022/01, January 5, 2022

ECORYS 2018
ECORYS, *Monitor anti-witwasbeleid 2014-2016: Eindrapportage*, onderzoek in opdracht van het WODC, September 2018

EDPS 2020
European Data Protection Supervisor, *Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing*, July 23, 2020

EDPS 2021
European Data Protection Supervisor, *Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals*, September 22, 2021

EDPS 2023
European Data Protection Supervisor, *EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations*, Ref: OUT2023-0017, March 28, 2023

European Parliament 2019
European Parliament, *Understanding money laundering through real estate transactions*, February 2019

European Commission 2019
European Commission, *Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institution,s* final, July 24, 2019

European Commission 2021
European Commission, *Report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)*, SEC(2021) 229 final - SWD(2021) 130 final, June 3, 2021

European Commission 2022
European Commission, *Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities,* COM(2022) 554 final, October 27, 2022

European Commission 2022a
European Commission, *Commission staff working document on the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing*, SWD(2022) 347 final, October 27, 2022

EY 2021
EY, *Onderzoek effecten Wwft: De effecten van de Implementatiewet vierde anti-witwasrichtlijn op Wwft-instellingen,* study commissioned by the Netherlands Ministry of Finance, July 2021

FATF 2016
FATF, *Mutual Evaluation Report of Italy,* February 2016

FATF 2017
FATF, *Guidance: Private sector information sharing*, November 2017

FATF 2018
FATF, *Life insurance sector: guidance for a risk-based approach,* October 2018

FATF 2019
FATF, *Guidance for a risk-based approach. Trust and company service providers,* June 2019

FATF 2019a
FATF, *Guidance for a Risk-Based Approach Guidance for Legal Professionals*, June 2019

FATF 2020
FATF, *Digital Identity*, March 2020

FATF 2021
FATF, *Opportunities and challenges of new technologies for AML/CFT*, July 2021

FATF 2021a
FATF, *Stocktake on data pooling, collaborative analytics and data protection*, July 2021

A. Bibliography

2. Reports

FATF 2021b
FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* October 2021

FATF 2022
FATF, *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing*, July 2022

FATF 2022a
FATF, *Risk-based Approach Guidance for the Real Estate Sector*, July 2022

FATF 2022b
FATF, *Mutual Evaluation Report of The Netherlands*, August 2022

FATF 2023
FATF, *Money Laundering and Terrorist Financing in the Art and Antiquities Market*, February 2023

FEC 2021
Financial Expertise Centre, *FEC Jaarverslag 2021,* April 5, 2022

FEC 2022
Financial Expertise Centre, *FEC Jaarverslag 2022,* April 4, 2023

FEC 2022a
Financial Expertise Centre, *FEC Jaarplan 2023,* December 20, 2022

FinCEN 2021
FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*, June 30, 2021

FIU 2021
FIU-the Netherlands, *Jaaroverzicht 2021*, July 2022

FIU 2023
FIU-the Netherlands, *Position paper: FIU-Nederland t.b.v. rondetafelgesprek over het Wetsvoorstel plan van aanpak witwassen,* January 26, 2023

German Federal Ministry of Finance 2020
German Federal Ministry of Finance, *Sicherheit: Sector-specific risk assessment 2020: Risk assessment of possible specific vulnerabilities of legal persons and other legal arrangements that could make them susceptible to being misused for ML/TF purposes*, December 2020

German Federal Ministry of Finance 2019
German Federal Ministry of Finance, *Sicherheit: First National Risk Assessment: Anti-Money Laundering/Countering the Financing of Terrorism 2018/2019*, October 2019

Government of Canada 2023
Government of Canada, *Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy 2023-2026*, March 2023

Government of Canada 2023a
Government of Canada, *Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*, March 2023

Hoogenboom 2021
A. B. Hoogenboom, *Samen: Samenwerking van notarissen, makelaars/taxateurs en overheidsinstellingen om witwassen en fraude bij onroerend goed transacties te voorkomen*, February 2021

ICAEW 2022
Institute of Chartered Accountants in England and Wales, *Accountancy AML Supervisors Group Risk Outlook*, April 2022

Institute of International Finance 2018
Institute of International Finance, *Machine Learning in Anti-Money Laundering – Summary Report*, October 2018

Irish Department of Finance 2019
Irish Department of Finance, *National Risk Assessment Ireland – Money Laundering and Anti-Terrorist Financing 2019*, April 2019

JFSC 2020
Jersey Financial Services Commission, *Exploring smart regulation: An assessment of the options for developing a shared KYC utility for the Jersey financial services sector*, July 2020

A. Bibliography

2. Reports

KPMG 2018
KPMG International, *Could blockchain be the foundation of a viable KYC utility?*, March 2018

KPMG 2021
KPMG, *Slimme technieken als antwoord op de Financial Economic Crime crisis*, May 5, 2021

KPMG 2022
KPMG, *De Glazen Leider: Hoe voorkomen we angst voor risico's in een tijd van zero tolerance*, May 2022

KPMG 2022a
KPMG, *Financial Crime - A Paradigm Shift*, November 2022

KPMG 2023
KPMG, *Trust in Artificial Intelligence. A global study,* February 2023

KPMG 2023a
KPMG, *Van invoering tot uitvoering. 5 jaar Algemene Verordening Gegevensbescherming (AVG) en het perspectief van de Nederlandse consument,* May 2023

Leung et al. 2022
D. Leung, B. Nolens, D. Arner and J. Frost, *Corporate digital identity: no silver bullet, but a silver lining*, BIS Papers No 126, June 2022

Maxwell 2021
N. Maxwell, *Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime,* Future of Financial Intelligence Sharing (FFIS) research programme, January 8, 2021

MEF 2019
Ministero dell'Economia e delle finanze, *Italy's national money laundering and terrorist financing risks assessment drawn up by the Financial Security Committee,* 2019

MEF 2020
Ministero dell'Economia e delle finanze, *Relazione al Parlamento sullo stato dell'azione di prevenzione del riciclaggio e del finanziamento del terrorismo, elaborata dal Comitato di sicurezza finanziaria*, 2020

Nationaal coördinator sanctienaleving and handhaving 2022
Stef Blok, *Rapport van de nationaal coördinator sanctienaleving en handhaving 2022*, May 21, 2022

National Bank of Belgium 2020
National Bank of Belgium, *Sectorale beoordeling van de witwasrisico's in de Belgische financiële sector die onder de toezichtsbevoegdheid van de Nationale Bank van België valt*, September 8, 2020

NVB (Netherlands Bankers' Association) 2019
Nederlandse Vereniging van Banken, *Position paper: Betrouwbaar UBO register essentieel voor aanpak witwassen en terrorismefinanciering*, May 2019

NVB 2022
Nederlandse Vereniging van Banken, *Position Paper: Information sharing*, June 2022

NVB 2022a
Nederlandse Vereniging van Banken, *Ongewenste effecten van de-risking voor klanten en banken*, September 26, 2022

NVB 2023
Nederlandse Vereniging van Banken, *Position paper: Wetsvoorstel plan van aanpak witwassen: Waarom banken met deze wetswijziging het misbruik van het financiële stelsel door criminelen beter kunnen voorkomen*, January 24, 2023

Openbaar Ministerie (Netherlands Public Prosecution Service) 2018
Openbaar Ministerie, *Onderzoek Houston: Feitenrelaas en Beoordeling Openbaar Ministerie*, September 4, 2018

Openbaar Ministerie 2021
Openbaar Ministerie, *Onderzoek Guardian: Feitenrelaas en Beoordeling Openbaar Ministerie*, April 19, 2021

Openbaar Ministerie 2022
Openbaar Ministerie, *Jaaroverzicht criminele geldstromen 2022*, April 12, 2023

A. Bibliography

2. Reports

RIEC-LIEC 2021
RIEC-LIEC, *Jaarverslag 2021*, July 7, 2022

RIEC The Hague 2022
RIEC The Hague, *Jaarverslag 2022,* April 7, 2023

Rijksuniversiteit Groningen (University of Groningen) 2023
Rijksuniversiteit Groningen, *Hoofdlijnen van de bestrijding van maffiacriminaliteit in Italië*, April 2023

RUSI 2016
RUSI, *Challenges to Information Sharing: Perceptions and Realities*, RUSI Occasional paper, July 8, 2016

RUSI 2017
N.J. Maxwell and D. Artingstall, *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime*, RUSI Occasional Paper, October 2017

RUSI 2018
RUSI, *Written Evidence to Economic Crime Inquiry: Anti-money laundering supervision and sanctions implementation*, ECR0018, May 2018

RUSI 2019
RUSI, *Deep impact? Refocusing the Anti-Money Laundering Model on Evidence and outcomes*, RUSI Occasional paper, October 11, 2019

RUSI 2022
RUSI, *Lessons in private-private financial information sharing to detect and disrupt crime,* Future of Financial Intelligence Sharing (FFIS), A Survey and Policy Discussion Paper, July 2022

SEO (Amsterdam Economics) 2021
Stichting Economisch Onderzoek, *Illegale trustdienstverlening: Een onderzoek naar de aard en omvang van de illegale trustsector in Nederland*, study commissioned by the Netherlands Ministry of Finance, January 2021

SEO 2022
Stichting Economisch Onderzoek, *De toekomst van de trustsector*, study commissioned by the Netherlands Ministry of Finance, October 11, 2022

Stichting Maatschappij en Veiligheid 2022
Stichting Maatschappij en Veiligheid, *Poortwachters tegen witwassen: Naar een poortwachters-functie van banken die beter bijdraagt aan voorkoming en bestrijding van witwassen*, June 20, 2022

Takáts 2007
E. Takáts, *A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement*, IMF Working Paper WP/07/81, April 2007

UIF 2021
Unità di Informazione Finanziaria per l'Italia, *Annual Report 2021,* May 2022

UK Finance 2018
UK Finance, *Written Evidence to Economic Crime Inquiry: Anti-money laundering supervision and sanctions implementation*, ECR0064, 2018

UK HM Government 2023
UK HM Government, *Economic Crime Plan 2023-2026*, March 2023

UK HM Treasury and Home Office 2019
UK HM Treasury and Home Office, *Economic Crime Plan 2019-2022*, July 2019

UK HM Treasury 2020
HM Treasury, *National risk assessment of money laundering and terrorist financing 2020*, December 17, 2020

UK Law Commission 2019
UK Law Commission, *Anti-money laundering: the SARs regime*, HC 2098 / Law Com No 384, 2019

UK Solicitors Regulation Authority 2021
UK Solicitors Regulation Authority, *Sectoral Risk Assessment - Anti-money laundering and terrorist financing*, January 28, 2021

Unger et al. 2006
B. Unger, G. Rawlings, M. Busuioc, J. Ferwerda, M. Siegel, W. de Kruijf and K. Wokke, *The amounts and the effects of money laundering*, report for the Ministry of Finance, February 16, 2006

A. Bibliography

2. Reports

Unger et al. 2013
B. Unger, H. Addink, J. Walker, J. Ferwerda, M. van den Broek and I. Deleanu, *The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy*, Project "ECOLEF" funded by the European Commission DG Home Affairs JLS/2009/ISEC/AG/087), February 2013

US Department of Treasury 2022
US Department of Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, May 2022

US Department of Treasury 2022a
US Department of the Treasury, *National Money Laundering Risk Assessment*, February 2022

Van Wingerde and Hofman 2022
K. van Wingerde and C. Hofman, *Wachters aan het woord: Dilemma's van accountants, advocaten, belastingadviseurs en notarissen in hun rol als poortwachter*, Politiekunde 116, 2022

Van Wingerde et al. 2023
K. van Wingerde, L. Bisschop and F. Brongers, *Onbedoeld ondermijnen: Verkennend onderzoek naar de wijze waarop de Nederlandse overheid onbedoeld de georganiseerde drugscriminaliteit kan faciliteren,* study commissioned by the Dutch Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), March 2023

Wolfsberg Group 2022
Wolfsberg Group, *Effectiveness through Collaboration*, June 21, 2022

Wolfsberg Group 2022a
Wolfsberg Group, *Wolfsberg Principles for Using Artificial Intelligence and Machine Learning in Financial Crime Compliance*, December 1, 2022

A. Bibliography

3. Media, press releases and blogs

N. Twomey, 'KYC Utilities: The Second Coming, Learning from Past Failures', *Finextra Blog* November 13, 2017

T. Lyman and L. de Koker, 'KYC Utilities and Beyond: Solutions for an AML/CFT Paradox', *CGAP Blog Series Beyond KYC Utilities* March 1, 2018

S. Merler, 'Latvia's money laundering scandal', *Bruegel Blog post* April 9, 2018

Openbaar Ministerie (Netherlands Public Prosecution Service), 'Trustkantoor Vistra betaalt 3,5 ton voor niet melden ongebruikelijke transacties', news release of September 3, 2019

R. Vaessen, 'Even een rekening openen', *Accountant.nl* September 6, 2019

Isabel Group, '4 grootbanken en Isabel Group bundelen krachten voor vereenvoudiging zakelijke dienstverlening met KUBE', press release of January 22, 2020

P. Ooms, 'KUBE: Blockchain voor banken', *FDmagazine.be* January 22, 2020

Invidem, 'Invidem partners with Encompass and iMeta Technologies to make KYC data handling easier', press release of April 6, 2020

Cetif Advisory, 'O-KYC, al via il progetto di Cetif Advisory', press release of July 22, 2020

S. Wass, 'Nordic banks' agreement on one KYC standard a 'unique advantage' for new utility', *S&P Global market intelligence* August 20, 2020

NVB, 'Nieuwe publiek-private samenwerking in Fintell Alliance - "Nieuwe boost voor aanpak witwassen"', news release of February 11, 2021

Cetif Advisory, 'Cetif - UniCatt insieme ad Intesa (Gruppo IBM) e CherryChain nel progetto Onboarding e Know Your Customer (O-KYC) su tecnologia DLT/Blockchain', press release of February 18, 2021

Australia Post, 'AusPost's Digital iD linked with DocuSign for e-signatures', press release of March 24, 2021

crime prevention with KYC utilities – interview with Invidem', *ThePaypers* June 25, 2021

FinCEN, 'FinCEN Issues First National AML/CFT Priorities and Accompanying Statements', press release of June 30, 2021

R. Betlem, 'Rabobank sluit kleine autodealers uit vanwege risico op witwassen', *FD (Netherlands Financieel Dagblad)* July 1, 2021

H.W. Smits and H. Rasch, 'Anti-witwasbeleid kost miljarden en levert weinig op', *FTM* July 8, 2021

European Commission, 'Anti-money laundering and countering the financing of terrorism legislative package', press release of July 20, 2021

E. Pastars, 'From zero to hero – a brief overview of AML evolution in Latvia', *Cobalt* September 10, 2021

FD (Netherlands Financieel Dagblad) Editorial, 'Banken voeren eenzame oorlog tegen witwassen', *FD* October 25, 2021

Politie (Netherlands Police), 'Serious Crime Taskforce leidt tot structurele samenwerking', press release of October 25, 2021

FIU-the Netherlands, 'FIU Nederland treedt samen met grootbanken op tegen witwassen en terrorismefinanciering', news release of November 2, 2021

Autoriteit Persoonsgegevens (Dutch Data Protection Authority), 'AP adviseert Eerste Kamer: neem WGS niet aan', press release of November 9, 2021

Rabobank, 'Rabobank heeft voorgenomen aanwijzing ontvangen van DNB', press release of November 16, 2021

Invidem, 'Invidem enters into an agreement with the first non-owner client', press release of April 19, 2022

'Kosten voor bankrekening blijven stijgen, ABN AMRO gooit er in een keer 51,3 procent bovenop', *Volkskrant* May 3, 2022

A. Bibliography

3. Media, press releases and blogs

HM Revenue & Customs and HM Treasury, 'Tax crime chiefs summit commits to international action', press release of May 13, 2022

CanDeal, 'Canadian Banks Partner with CanDeal to Deliver Industry-wide KYC Solution', press release of June 27, 2022

G. Stack, 'Latvian Prosecutors Charge Bankers with Laundering 2.1B Euro', *OCCRP* July 29, 2022

'ING te druk met witwasonderzoek, weert stichtingen en verenigingen', *NOS.nl* August 29, 2022

R. Betlem, 'Zakelijke rekeningen duurder door stijgende kosten witwasonderzoek', *FD* August 30, 2022

Intesa, 'Progetto O-KYC, inizia la fase due', press release of October 5, 2022

DNB, 'MiCAR belangrijke stap in regulering van crypto-markten', news release of October 6, 2022

Autoriteit Persoonsgegevens, 'Nieuwe wet opent deur naar ongekende massasurveillance door banken', press release of October 21, 2022

A. Ploumen, KNB: 'Onderlinge gegevensdeling tegen witwassen nodig en gewenst', *MrOnline* November 7, 2022

'Banken weigeren goede doelen om 'witwasrisico'', *RTL Nieuws* November 15, 2022

DNB, 'Partijen voortvarend van start met gerichte risicogebaseerde witwasaanpak', news release of November 23, 2022

N. Boere, 'Online gokken als witwasmethodiek', news release of AMLC November 28, 2022

Ministerie van Buitenlandse Zaken | Expertisecentrum Europees recht (Netherlands Ministry of Foreign Affairs | European law Expertise Centre), 'EU-regeling voor onbeperkte toegang van het publiek tot informatie over de uiteindelijk begunstigden van vennootschappen is ongeldig', news release of December 2, 2022

'Bedrijven, stichtingen en kerken moeten van banken meebetalen aan witwasonderzoek', *NOS.nl* December 27, 2022

R. Betlem and M. Rotteveel, 'Machine tegen witwassen werkt niet', *FD* 10 January 2023
A. Clare, 'Sanctions screening regtech GSS secures $45mn in funding', *Fintech Magazine* January 23, 2023

Verbond van Verzekeraars, 'Meer duidelijkheid toegang UBO-register', news release of January 24, 2023

C. de Horde, R. Betlem, 'Felle verdeeldheid onder voor- en tegenstanders van nieuwe witwaswet', *FD* January 26, 2023

European Commission, 'The European Digital Identity Wallet Architecture and Reference Framework', news release of February 10, 2023

'Nederland kent strengste trustwetgeving in EU', *Holland Quaestor* February 27, 2023

Rijksoverheid, 'Eerste Kamer neemt Wet digitale overheid aan', news release of March 21, 2023

G. de Groot, J. Leupen and S. Motké, 'Russische klanten gaan ondergronds na Nederlands trustverbod', *FD* March 24, 2023

S. Motké, G. de Groot and J. Leupen, 'Hoe een 'zwart gat' in Amsterdam zich vult met Russen', *FD* March 24, 2023

FD Redactioneel Commentaar, 'Nederland heeft blinde vlek in trusttoezicht', *FD* March 28, 2023

College voor de Rechten van de Mens (Netherlands Institute for Human Rights), 'Verzoek geweigerd – Mogen banken klanten afwijzen op grond van nationaliteit?', news release of April 4, 2023

K. van Doorne, 'Met knikkende knieën ongebruikelijke transacties melden? Dat kan toch niet', column *VNO-NCW*, April 5, 2023

NVB (Netherlands Bankers' Association) , 'Openheid en transparantie in uitvoering anti-witwaswet', news release of April 6, 2023

A. Bibliography

3. Media, press releases en blogs

'Racismecoördinator: 'Structurele discriminatie van moslims bij banken', *NOS.nl* April 6, 2023

M. Pols, E. van der Schoot, 'OM-topman: 'Ik mis de verontwaardiging over criminaliteit die het bedrijfsleven ondermijnt'', *FD* April 21, 2023

Council of the EU, 'Council adopts new rules on markets in crypto-assets (MiCA)', press release of May 16, 2023

Council of the EU, 'Anti-money laundering: Council adopts rules which will make crypto-asset transfers traceable', press release of May 16, 2023

NVB, 'Minder klantimpact door NVB Standaarden voor risicogebaseerd witwasonderzoek', press release of May 30, 2023

'Onderzoek: Italiaanse maffia-aanpak deels bruikbaar voor Nederland', *NOS.nl* June 7, 2023

I. Withers and K. Ridley, 'BREAKING: Six British banks to share fincrime information in a 'game changer' plan to crack down on money laundering; Lloyds, NatWest already involved in trials', *AMLIntelligence* June 22, 2023

Council of the EU, 'Russia's war of aggression against Ukraine: EU adopts 11th package of economic and individual sanctions', press release of June 23, 2023

A. Bibliography

4. Parliamentary Documents

Kamerstukken (Netherlands Parliamentary Documents) I, 2022/2023, 31 477 and 34 08, D[1] (the letter D only relates to 31 477)

Kamerstukken I, 2022/2023, 35 447, K

Kamerstukken II, 2007/2008, 31 237 and 31 238, no. 6

Kamerstukken II, 2007/2008, 31 238, no. 3

Kamerstukken II, 2017/2018, 29 911, no. 180

Kamerstukken II, 2017/2018, 34 808, no. 3

Kamerstukken II, 2017/2018, 34 910, no. 3

Kamerstukken II, 2018/2019, 31 477, no. 41, annex plan van aanpak witwassen

Kamerstukken II, 2020/2021, 31 477, no. 60, annex

Kamerstukken II, 2021/2022, 29 911, no. 348

Kamerstukken II, 2021/2022, 36 085, no. 2

Kamerstukken II, 2021/2022, 36 102, no. 3

Kamerstukken II, 2022/2023, 31 477, no. 80

Kamerstukken II, 2022/2023, 32 545, no. 180

Kamerstukken II, 2022/2023, 36 200 V, no. 56

Kamerstukken II, 2022/2023, 36 045, no. 120

Kamerstukken II, 2022/2023, 36 228, no. 2.

Kamerstukken II, 2022/2023, 36 228, no. 3

Kamerstukken II, 2022/2023, Appendix to the Proceedings, 2595

A. Bibliography

5. Enforcement decisions of regulators

AFM (Dutch Authority for the Financial Markets), *Aanwijzing STX Fixed Income B.V.*, June 8, 2021, available via this link

AFM, *Bestuurlijke boete FlatexDeGiro*, December 23, 2021, available via this link

AFM, *Aanwijzing Zwaan Finance B.V.*, March 25, 2022, available via this link

AFM, *Bestuurlijke boete Robeco Institutional Asset Management B.V.*, March 31, 2022, available via this link

AFM, *Bestuurlijke boetes Revo Capital Management B.V.*, May 25, 2022, available via this link

Autoriteit Persoonsgegevens (Dutch Data Protection Authority), *Boete TikTok vanwege schenden privacy kinderen*, July 21, 2021, available via this link

Autoriteit Persoonsgegevens, *Boete Belastingdienst voor discriminerende en onrechtmatige werkwijze*, December 7, 2021, available via this link

DNB (The Dutch Central Bank), *Bestuurlijke boete Suri-Change B.V.*, November 25, 2014, available via this link

DNB, *Aanwijzing MUFG Bank (Europe) N.V.*, July 29, 2019, available via this link

DNB, *Bestuurlijke boete JTC Institutional Services Netherlands B.V.*, June 14, 2021, available via this link

DNB, *Bestuurlijke boete Travelex N.V.*, February 2, 2023, available via this link

A. Bibliography

6. Court decisions

EU Court of Justice, November 22, 2022, C-37/20 and C-601/20, ECLI:EU:C:2022:912 (*WM v Luxembourg Business Registers* and *Sovim v Luxembourg Business Registers*)

CBb (Netherlands Trade and Industry Appeals Tribunal), March 3, 2020, ECLI:NL:CBB:2020:120

CBb, October 18, 2022, ECLI:NL:CBB:2022:707 (*Bunq*)

The Hague Court of Appeal, February 1, 2019, ECLI:NL:GHDHA:2019:187

Amsterdam Court of Appeal, January 21, 2020, ECLI:NL:GHAMS:2020:121

District Court of Amsterdam, December 1, 2020, ECLI:NL:RBAMS:2020:6245

District Court of Amsterdam, April 22, 2021, ECLI:NL:RBAMS:2021:2600

District Court of Amsterdam, January 5, 2022, ECLI:NL:RBAMS:2022:42

District Court of Amsterdam, June 15, 2022, ECLI:NL:RBAMS:2022:3871

District Court of Amsterdam, September 14, 2022, ECLI:NL:RBAMS:2022:5340

Kamer voor het notariaat (Chamber for Notarial Matters), Amsterdam, March 10, 2022, ECLI:NL:TNORAMS:2022:8

Kamer voor het notariaat, The Hague, May 25, 2022, ECLI:NL:TNORDHA:2022:10

Kamer voor het notariaat, The Hague, July 15, 2022, ECLI:NL:TNORDHA:2022:14

Kamer voor het notariaat, Den Bosch, September 19, 2022, ECLI:NL:TNORSHE:2022:31

A. Bibliography

7. Websites

AMLC, *Strafrechtelijke aanpak via de Wwft*, available via this link

AMLC, *Wat wil het AMLC bereiken*, available via this link

AMLC, *Wie zijn wij en wat doen wij*, available via this link

AUSTRAC, *Reliable and independent documentation and electronic data*, available via this link

Australia Post, *AML solutions: Digital iD AML/KYC offering*, available via this link

Australia Post, *Digital ID*, available via this link

Banca d'Italia, *Regulatory sandbox: admitted projects*, available via this link

Currence, *Collectieve betaalproducten: IDIN*, available via this link

DNB, *Q&A Elektronische identificatiemiddelen en cliëntidentificatie*, available via this link

DNB, *Sanctiescreening*, 16 September 2022, available via this link

Eerste Kamer (Netherlands Senate), *Initiatiefvoorstel-Nijboer en Alkaya Wet centraal aandeelhoudersregister*, available via this link

European Parliament, *Artificial intelligence: Threats and opportunities*, available via this link

European Commission, *The European Commission's priorities*, available via this link

European Commission, *Digital identity for all Europeans*, available via this link

European Commission, *European digital identity*, available via this link

Europol, *European Financial and Economic Crime Centre – EFECC*, available via this link

FIU-the Netherlands, *Ik heb een melding gedaan: wat nu?*, available via this link

FIU-the Netherlands, *Nationale samenwerking,* available via this link

iDIN, *iDIN – Een veilig iD*, available via this link

i-Hub, *About i-Hub*, available via this link

Monetary Authority of Singapore, *Digital ID and e-KYC*, available via this link

National Crime Agency, *National Economic Crime Centre*, available via this link

NVB (Netherlands Bankers' Association), *IVR/EVR-registratie*, available via this link

Rijksinspectie Digitale Infrastructuur, *Elektronische vertrouwensdiensten*, available via this link

Rijksoverheid (Netherlands State Government), *Digitale Overheid*, available via this link

Singpass, *MyInfo: speed up eKYC processes for individual users with data from government sources*, available via this link

Singpass, *Singpass API Products*, available via this link

Singpass, *Transforming Singapore through technology*, available via this link

TMNL, *Ethische commissie*, available via this link

TMNL, *Over TMNL*, available via this link

TMNL, *TMNL in het kort: Samen financiële criminaliteit bestrijden*, available via this link.

A. Bibliography

8. Miscellaneous

Autoriteit Persoonsgegevens (Dutch Data Protection Authority), *Besluit inzake de vergunningaanvraag voor de verwerking van [PARTIJ] volgens het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021*, August 20, 2021, kenmerk z2021-03355, available via this link

Belastingdienst Bureau Toezicht Wwft, *Leidraad Wwft voor makelaars, bemiddelaars en taxateurs onroerende zaken*, March 2022, available via this link

Coalitieakkoord 2021-2025*, Omzien naar elkaar, vooruitkijken naar de toekomst*, December 15, 2021, available via this link

Consultatie voor de Wijzigingswet financiële markten 2024, April 29, 2022, available via this link

Consultatie voor het Besluit gegevensverwerking door samenwerkingsverbanden, February 20, 2023, available via this link

Consultatie voor de Wijzigingswet beperking toegang UBO-registers, May 30, 2023, available via this link

DNB (the Dutch Central Bank), *Leidraad Wwft/Sw,* September 2022, available via this link

European Banking Authority, *Guidelines on the role of AML/CMT compliance officers*, EBA/GL/2022/ 05, June 14, 2022, available via this link

European Banking Authority, *Guidelines on remote customer onboarding*, EBA/GL/2022/15, November 22, 2022, available via this link

Goede Doelen Nederland, *Tweede brandbrief aan Kaag over gevolgen de-risking banken*, April 21, 2022, available via this link

Ministerie van Financiën (Netherlands Ministry of Finance), *Leidraad Financiële Sanctieregelgeving*, August 12, 2020, available via this link

Monetary Authority of Singapore, *Circular AMLD 01/2018: Use of MyInfo and CDD Measures for Non Face-to-Face Business Relations*, January 8, 2018, available via this link

Monetary Authority of Singapore, *Circular ID 26/20: Outsourcing arrangements involving services wholly provided by the Government Technology Agency ("GovTech") or agents appointed by GovTech*, June 9, 2020, available via this link

Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021 (PIFI 2021), available via this link

Reactie van NVM, VBO en VastgoedPro op het wetsvoorstel Wet plan van aanpak witwassen, 2020, available via this link

Wetenschapstoets wetsvoorstel Plan van Aanpak Witwassen, January 20, 2023, available via this link.

Initiatives in the Netherlands and abroad

B

B. Initiatives in the Netherlands and abroad

1. Information sharing between gatekeepers

1.1. Transactie Monitoring Nederland (TMNL)

Transactie Monitoring Nederland ('TMNL') was established on July 10, 2020 by ABN AMRO Bank, ING Bank, Rabobank, Triodos Bank and de Volksbank.(407) It was incorporated as a private limited company in which the participating banks are shareholders.(408) It is a collective transaction monitoring utility. Currently, TMNL's work is limited to the participating banks, but in the long term the intention is that other financial institutions can also be served by TMNL.(409)

In TMNL, the participating banks bring together their transaction data on corporate customers with the objective of identifying unusual patterns in payment transactions that are not exposed when the banks monitor transactions individually. This approach enables money laundering networks and potential attempts in that regard to be identified and appropriate action to be taken.(410) With the ability to establish connections and jointly monitor transaction patterns "*criminals can less easily exploit the 'dark space' between banks.*"(411)

TMNL is in a *minimum viable product phase* and operates within the current legal constraints.(412) For it to take the next step, a number of aspects of the Wwft need to be amended, in particular by creating a legal basis for collective transaction monitoring.(413) Sections 3.2.1 and 3.2.5 of the study report have already discussed the Bill on the Money Laundering Action Plan, which is to provide this legal basis.

In the current phase, TMNL conducts all its analytical activities in addition to the banks' own monitoring activities. TMNL limits itself to transactions involving (accounts held with) multiple banks and it focuses entirely on detecting unusual transaction patterns, for which it uses sophisticated analytical models. When it identifies unusual patterns, it feeds them back individually in the form of alerts to the banks involved. The participating banks themselves process these alerts and take any follow-up action needed, such as reporting unusual transactions.(414)

For privacy reasons, it was decided that TMNL would only monitor corporate customer transactions. TMNL only receives information that is strictly necessary (data minimization). The banks pseudonymize the transaction and customer data they disclose to TMNL.(415) This means that information traceable to particular entities such as company name and account number is converted to an irreducible string of characters. TMNL is also careful to handle the analytical models responsibly and ethically. The organization has an ethics committee composed of academics who objectively advise TMNL on the ethical issues involved in the use of such models.(416)

Although TMNL is a private initiative, it collaborates with other bodies such as FIU-NL and the AMLC.(417) The purpose of this is to create risk indicators for money laundering and terrorist financing and to share information about the *modus operandi* of criminals. This information is incorporated into TMNL's detection models.(418)

(407) TMNL, *About TMNL*, available via this link.
(408) FATF 2022, p. 27.
(409) TMNL, *TMNL in het kort: Samen financiële criminaliteit bestrijden*, available via this link.
(410) NVB 2023; Diepenmaat 2021, p. 126.
(411) NVB 2023, p. 5.
(412) FATF 2022, pp. 26-27.
(413) Bill on the Money Laundering Action Plan, Parliamentary Papers II, 2022/2023, 36 228, no. 2.
(414) FATF 2022, pp. 26-27.
(415) FATF 2022, pp. 26-27.
(416) TMNL, *Model ethics committee*, available via this link.
(417) TMNL, *TMNL in het kort: Samen financiële criminaliteit bestrijden*, available via this link; FIU 2023, pp. 1-2.
(418) FIU 2023, p. 2.

B. Initiatives in the Netherlands and abroad

TMNL and the Financial Intelligence Unit-Netherlands ('FIU-NL') also conducted a joint pilot project within Fintell Alliance in 2021. Based on this pilot, FIU-NL concluded that the benefits of collective transaction monitoring include better and more complete unusual transaction reports to FIU-NL and heightened prevention of (rogue) customers' shopping behavior.(419) In addition, alerts about criminals' *modus operandi* shared by FIU-NL and included in TMNL's models produce faster results than those obtained by individual banks using their models to process such *modus operandi* and risk indicators.(420)

1.2. Know Your Customer Utility for Banks and Enterprises (KUBE)

Short for 'Know Your Customer Utility for Banks and Enterprises', KUBE is an initiative of Belgium's four major banks Belfius, BNP Paribas Fortis, ING Belgium and KBC together with fintech company Isabel Group.(421) The initiative was launched in January 2020. No new parties have joined KUBE since then.

KUBE focuses on simplifying the KYC process of the banks' shared corporate customers when entering into a business relationship and when conducting ongoing monitoring. One of its objectives is to improve the efficiency of this process: with customer consent, organizational data provided to one bank as part of customer due diligence may subsequently be shared with other member banks: "*[w]hen a company opens an account with another bank, the KYC process will be more rapid as the required data will already be available. The company will therefore be able to open accounts without being subject to red tape and delays.*"(422) The parties involved share customer data with each other using blockchain. This means that data is not stored in a central database. The KUBE blockchain application is operated by Isabel Group.

In practice, KUBE works as follows: a corporate customer provides the requested KYC data to the bank where it wants to purchase services using the KUBE application. That bank verifies the data according to the verification rules agreed between the banks. With the customer's authorization, the KYC data and verification status of each piece of information are entered into KUBE. When other banks establish a business relationship with the same customer, they can then retrieve the relevant KYC data and verification status and use them for their own KYC research. The bank that first verified the corporate customer's KYC data receives payment from the other banks that use that data.(423) All participants pay subscription fees to Isabel Group for their use of KUBE.

According to its website, KUBE is fully GDPR-compliant because of its 'privacy-by-design' principle and the use of blockchain technology, which does not store customers' business data in a central database. An important aspect is that customer consent is sought for sharing information.(424)

1.3. Invidem Nordic KYC utility

A not-for-profit enterprise, Invidem AB was launched by six Scandinavian banks in 2019. The participating banks are Danske Bank, DNB, Handelsbanken, Nordea, SEB and Swedbank, which hold joint ownership of the entity. Invidem launched its KYC platform in September 2021. In April 2022, Invidem expanded for the first time, incorporating a Swedish fund management company.(425)

(419) FIU 2023, p. 2.
(420) FIU 2023, p. 2.
(421) Isabel Group, 'Four major banks and Isabel Group join forces to streamline business services with KUBE', press release January 22, 2020.
(422) P. Ooms, 'KUBE: Blockchain voor banken', *FDmagazine.be* January 22, 2020.
(423) Information compiled, translated and summarized by KPMG from the website https://www.kube-kyc.be/en/.
(424) Information compiled, translated and summarized by KPMG from the website https://www.kube-kyc.be/en/.
(425) Invidem, 'Invidem enters into an agreement with the first non-owner client', press release April 19, 2022.

B. Initiatives in the Netherlands and abroad

However, in April 2023, Invidem announced on its website that it would shut down.

Invidem's Nordic KYC utility is a platform for corporate customers using a data standard pre-agreed and harmonized by the banks. The platform is used to collect and verify KYC data and to validate general data. Invidem has thus also called itself a 'clearing house for KYC information'.(426)

Corporate customers' data is stored in a centralized location, with the customer being able to control which party gets access to which information.(427) The KYC utility can be used both for onboarding and during the course of a relationship.

Before Invidem announced that it was shutting down, the common KYC data standard and the strong commitment of the founding banks were identified as key success factors.(428) In a 2021 interview, Invidem's CEO said that using the utility would offer customers a number of advantages, including not having to repeatedly provide their information (partly due to the harmonized data standard), better control over their own continuously updated KYC data and faster access to financial services. The advantages for participating parties would include reduced times to complete customer due diligence (in part due to automatic data collection), dependability of the data supplied and up-to-date customer files.(429) In its online announcement of its shutdown, Invidem noted that the rapid development of laws and regulations as well as technological advances had increased the level of complexity beyond what it had originally envisaged. This also made achieving the desired economies of scale more difficult for both customers and banks.(430)

1.4. O-KYC

In Italy, a project called 'O-KYC' has been running since June 2020. After an initial testing phase that ended in February 2021, the project was admitted to the Italian Central Bank's regulatory sandbox for an 18-month period.(431) A regulatory sandbox is a controlled testing environment that enables innovative products and services to be developed and validated. Such products and services are often not (entirely) allowed under the current legal framework. However, this can be temporarily waived because the products and services in question are not being provided to customers.

Participants in the O-KYC project are Cetif Advisory(432), CherryChain (fintech) and Intesa (IBM Group), as well as the following six Italian banks: Banca IFIS, Banca Mediolanum, Banca Popolare di Puglia e Basilicata, Cherry Bank, Iccrea Banca and Banca Monte dei Paschi di Siena. The project also includes a law firm, which oversees the project's legal aspects.(433)

O-KYC focuses on the onboarding phase of the KYC process and its main objective is to simplify this process in order to reduce time and expense and to improve the efficiency of gatekeepers' internal processes.(434) It also impacts the customer experience, as it eliminates the need for the repeated submission of identical or similar data to different gatekeepers.

(426) S. Wass, 'Nordic banks' agreement on one KYC standard a 'unique advantage' for new utility', *S&P Global market intelligence* August 20, 2020.
(427) Invidem, 'Invidem partners with Encompass and iMeta Technologies to make YC data handling easier', press release April 6, 2020.
(428) M. Ciobanu, 'Interview Advancing modern financial crime prevention with KYC utilities – interview with Invidem', *ThePaypers* June 25, 2021.
(429) M. Ciobanu, 'Interview Advancing modern financial crime prevention with KYC utilities – interview with Invidem', *ThePaypers* June 25, 2021.
(430) www.invidem.com.
(431) Banca d'Italia, *Regulatory sandbox: admitted projects*, available via this link.
(432) Cetif Advisory is a spin-off of Cetif, the Università Cattolica del Sacro Cuore's research center.
(433) Cetif Advisory, 'Cetif - UniCatt insieme ad Intesa (Gruppo IBM) e CherryChain nel progetto Onboarding e Know Your Customer (O-KYC) su tecnologia DLT/Blockchain', press release February 18, 2021.
(434) Cetif Advisory, 'O-KYC, al via il progetto di Cetif Advisory', press release July 22, 2020.

B. Initiatives in the Netherlands and abroad

Public sources do not clarify whether the project targets corporate customers, natural persons or both; however, the fact that it operates via an app implies that it at least trains its sights on natural persons. In practice, the aim is for any of the participants (the 'custodian') to create a 'KYC wallet' for customers. With that customer's consent, the information contained in the wallet can be shared with other participants who request the information (the 'requesting parties'). Distributed Ledger Technology (DLT) and blockchain technology play a major role in the system that is being set up to exchange the data. The project is also looking at a possible custodian fee in the form of 'tokens' that can be spent within the system.(435)

According to the parties involved, the O-KYC system is GDPR-compliant. In particular, end users (i.e. customers) have control over their own data and the system's internal processes are secured.(436)

1.5. i-Hub KYC Repository for Ongoing Due Diligence

The KYC Repository for Ongoing Due Diligence was rolled out in Luxembourg in December 2019. This commercial platform is operated by i-Hub. i-Hub is a subsidiary of Post Luxembourg (a state-owned company) and BGL BNP Paribas.(437) It is licensed as a support professional of the financial sector (a 'support PFS') and is supervised by Commission du Surveillance du Secteur Financier (CSSF), the Luxembourg financial regulator.(438)

Strictly speaking, the i-Hub KYC Repository is not a KYC utility; by using the KYC Repository for Ongoing Due Diligence, affiliated gatekeepers effectively outsource their customer due diligence to i-Hub. For now, the platform focuses primarily on banks, investment fund (managers) and investment firms.

The KYC Repository is a centralized platform that stores data on customers (both natural persons and legal entities) and related parties. i-Hub has a standardized data model and, on behalf of the affiliated gatekeepers, validates data received from customers and information from public registers (e.g. the Business Register and UBO register). Updates to these public registers are automatically incorporated into the tool and included in customer profiles. The platform can also be used to carry out PEP and sanctions screening, including handling alerts, as well as to perform customer risk weighting and assessment. On the basis of service level agreements, it is also tailored to individual needs of each affiliated gatekeeper. The platform does not, however, include transaction monitoring.(439)

It does allow information sharing among affiliated gatekeepers, which is based on the consent of the customer, or end user ('opt-in'). Updates of customer information are sent to all the end user's business contacts through the platform.(440)

(435) Cetif Advisory, 'O-KYC, al via il progetto di Cetif Advisory', press release July 22, 2020.
(436) Cetif Advisory, 'Cetif - UniCatt insieme ad Intesa (Gruppo IBM) e CherryChain nel progetto Onboarding e Know Your Customer (O-KYC) su tecnologia DLT/Blockchain', press release February 18, 2021.
(437) i-Hub, *About i-Hub*, available via this link.
(438) One feature of a support PFS is that it does not provide a financial service or activity itself, but rather performs certain operational functions on behalf of other financial institutions and service providers.
(439) Information compiled, translated and summarized by KPMG from the website https://www.i-hub.com/b2b/.
(440) Information compiled, translated and summarized by KPMG from the website https://www.i-hub.com/b2b/.

B. Initiatives in the Netherlands and abroad

1.6. Legislation regarding KYC utilities in Latvia

In 2022, Latvia introduced legislation designed for the set-up and use of KYC utilities.(441) This legislation is part of the Latvian Action Plan for the Prevention of Money Laundering and Terrorist Financing 2020-2022,(442) which was developed in response to MONEYVAL's negative evaluation of Latvia's anti-money laundering policy and heightened international monitoring of the country shortly thereafter. Around the same time, there were also issues at ABLV Bank, one of Latvia's largest banks,(443) which the U.S. authorities suspected of money laundering and helping customers evade sanctions imposed on North Korea. In the summer of 2022, Latvian authorities announced the prosecution of senior executives of the bank, which by then had already been liquidated.(444)

New legislation in Latvia allows gatekeepers to use KYC utilities to improve the effectiveness and efficiency of their customer due diligence. The purpose of the legislation is to promote information sharing between gatekeepers who do not belong to the same legal group.(445) The legislation provides two options for the set-up of a shared KYC utility and sets out the corresponding powers. It also facilitates the establishment of a joint KYC utility and sets out a licensing and supervisory regime in that regard.

Under the legislation, the KYC utility is allowed to be in two versions: a closed and an open variant. At the time of the study, no licensed KYC utilities were operating in Latvia.

Closed shared KYC utility

A closed shared KYC utility is one created by gatekeepers on a contractual basis and managed by an external service provider. Part of the KYC process can be outsourced to this service provider, provided that this is in line with competition law.(446) The new legislation in force allows different categories of gatekeepers that do not belong to the same legal group to jointly outsource (aspects of) the KYC process.(447) However, this has to be in conformity with competition law.(448)

Open shared KYC utility

An open shared KYC utility is a platform operated by an independent service provider from which gatekeepers can obtain information about customers and their UBOs for their customer due diligence. Compared to closed utilities, much more data is shared that comes from both private and public sources (e.g. government registers). To prevent gatekeepers from being held legally liable for providing information in good faith in an open shared KYC utility, the law stipulates that the provision of such information is not considered disclosure of confidential information.(449)

(441) See Section 17 of the Latvian *Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing* (June 13, 2019), available via this link (herainafter: the 'Latvian AML/CFT Act'); and the Latvian *Regulations Regarding the Requirements for Updating Information in the Shared Know-Your-Customer Utility and the Licensing and Supervision of the Shared Know-Your-Customer Utility Service Provider (Cabinet Regulation No. 396)*, available via this link (hereinafter: the 'Latvian KYC Utility Regulations').

(442) In December 2022, the Latvian government adopted the Action Plan for the Prevention of Money Laundering, Terrorism and Proliferation Financing 2023-2025: Latvian Ministry of the Interior, *Strengthening Latvia's capacity to combat financial crime*, press release December 16, 2022, available via this link.

(443) E. Pastars, 'From zero to hero – a brief overview of AML evolution in Latvia', *Cobalt* September 10, 2021; *Cabinet of Ministers, Order no. 122 On the action plan for the prevention of money laundering, terrorism and proliferation financing for 2022*, available in the official language via this link.

(444) S. Merler, 'Latvia's money laundering scandal', *Bruegel Blog post* April 9, 2018; G. Stack, 'Latvian Prosecutors Charge Bankers with Laundering 2.1B Euro', *OCCRP* July 29, 2022.

(445) Annotation to an amendment of the Latvian AML/CFT Act, No. 90/TA-1880 (2020), part I(2)(10) *Initial Impact Assessment*, available via this link.

(446) Section 17.1(1) of the Latvian AML/CFT Act.

(447) Annotation to an amendment of the Latvian AML/CFT Act, No. 90/TA-1880 (2020), part I(2)(10) *Initial Impact Assessment*, available via this link.

(448) Annotation to an amendment of the Latvian AML/CFT Act, No. 90/TA-1880 (2020), part I(2)(10) *Initial Impact Assessment*, available via this link.

(449) Section 17.2(5) of the Latvian AML/CFT Act.

B. Initiatives in the Netherlands and abroad

The following information may be processed in an open shared KYC utility:[450]

1. Publicly available information.
2. Customer information about legal entities or UBOs that is obtained from government systems containing confidential data (excluding information on criminal convictions); gatekeepers are required to collect such information under anti-money laundering regulations.
3. Information shared by gatekeepers within the current legal framework for introductory customer due diligence,[451] or affiliated gatekeepers in the same category being informed that a report has been made to the FIU regarding a joint customer and transaction.[452]
4. Information about parties subject to sanctions but not directly mentioned on international sanctions lists (sectoral sanctions), as well as on legal entities used to circumvent international sanctions.
5. Information about a natural person collected as part of the customer due diligence process for which that person has consented for it to be shared through the open shared KYC utility.

Information sharing within the open shared KYC utility creates the opportunity for customers to use the one-stop principle. After giving consent for their data to be shared, the customer no longer has to provide it to each gatekeeper.[453] The customer is free to withdraw this consent if they so wish.[454]

The information exchanged through open shared KYC utilities is directly accessible to the Latvian FIU. Any access to information by other government agencies needs to be regulated by law.[455]

Authorization and supervision

Closed shared KYC utilities where gatekeepers do not belong to the same financial or legal group, and all open shared KYC utilities, are subject to a licensing requirement. The Latvian privacy regulator (Datu valsts inspekcija) is designated as the regulator of these KYC utilities and is responsible for licensing. Licenses are issued to the service providers who are to operate the KYC utility (or platform, as the case may be) and are valid for five years.[456] To obtain a license, service providers must satisfy several conditions. For example, the service provider may not have a tax debt. To ensure GDPR compliance, the service provider has to have appointed a privacy officer. Furthermore, the service provider's shareholders and directors are required to have a good reputation and the appropriate education. Another example is that the service provider must have appropriate liability insurance.[457]

1.7. CanDeal industry-wide KYC Solution

In June 2022, CanDeal, an operator of Canadian market and infrastructure services, announced plans to partner with five Canadian banks to create a centralized KYC solution for the capital markets sector.[458]

(450) Section 17.2(3) of the Latvian AML/CFT Act.
(451) Section 29 of the Latvian AML/CFT Act.
(452) Section 38(4) of the Latvian AML/CFT Act.
(453) Annotation to an amendment of the Latvian AML/CFT Act, No. 90/TA-1880 (2020), part I(2)(10) *Initial Impact Assessment*, available via this link.
(454) Section 6 of the Latvian KYC Utility Regulations.
(455) Section 17.2(6) of the Latvian AML/CFT Act.
(456) Section 17.3 of the Latvian AML/CFT Act.
(457) For all conditions, see Sections 8-16 of the Latvian KYC Utility Regulations.
(458) CanDeal, 'Canadian Banks Partner with CanDeal to Deliver Industry-wide KYC Solution', press release June 27, 2022.

B. Initiatives in the Netherlands and abroad

The participating banks are Bank of Montreal, Bank of Nova Scotia (Scotiabank), Canadian Imperial Bank of Commerce, National Bank of Canada and Royal Bank of Canada. The goal is to achieve common data agreements, leading to greater confidence in the use of data in risk assessments and a more streamlined KYC process for customers.

1.8. Incident Warning System for Financial Institutions (IFI)

The Incident Warning System for Financial Institutions (IFI) is the system that allows financial institutions to investigate whether someone - for example, a customer or employee - is or could be a threat to the institution or the financial sector. Participants are banks, insurers, mortgage lenders and finance companies licensed under financial laws and regulations to provide services in the Netherlands, and which are members of the participating industry associations.(459)

The IFI consists of the internal reference indexes, or incident registers ('IVR'), and the external reference index ('EVR'). These are registers held by banks and insurers and their industry associations that contain information on customers and employees involved in incidents such as fraud, money laundering or forgery.(460)

The IVR is the internal register used by a financial institution (or group of such institutions) that contains records of persons who have been involved in an incident within that institution. Internal registers are accessible to the financial institution's staff and contain the name and date of birth of natural persons or the Chamber of Commerce number of legal entities (and possibly also their company name and zip code). Only the Security Department is aware of the nature and background of the incident.(461) Every institution must have an incident register and is a data controller pursuant to privacy regulations.

Linked to the incident register, the external reference index is shared among financial institutions and contains records of customers involved in serious incidents. Banks and insurers thus have access to information about customers of other financial institutions. Information recorded in the external reference index is also retained in an institution's incident register. The institution itself is the controller for data processing purposes.

For an entry in internal registers, it is sufficient that an event has occurred that the institution believes poses a risk or needs attention. For entries in an external register, however, more serious suspicion is required, involving events that could threaten the institution, its employees or the financial sector. It has to be established with a level of certainty that the relevant natural person or legal entity is involved in the event or threat. This means that, in principle, criminal offences can be reported and that more than just a reasonable suspicion of guilt is required.(462)

The registers can be accessed through the computer system known as 'EVA'.(463) A register check is therefore called an 'EVA test'. In the case of natural persons, employees enter the name and date of birth of a prospective customer after which they are notified whether or not that person is listed in the incident register or external reference index ('hit/no hit').

(459) The participating industry associations are: The Dutch Banking Association (*Nederlandse Vereniging van Banken*; NVB), the Dutch Association of Insurers (*Verbond van Verzekeraars*), the Dutch Finance Houses' Association (*Vereniging van Financieringsondernemingen in Nederland*; VFN), the Dutch Foundation for the Prevention of Mortgage Fraud (*Stichting Fraudebestrijding Hypotheken*; SFH) and the Association of Dutch Healthcare Insurers *(Zorgverzekeraars Nederland*; ZN). Financial institutions that are not members of the NVB, the Dutch Association of Insurers, or ZN may also be admitted as participants under strict conditions.

(460) NVB, *IVR/EVR registratie*, available via this link.

(461) NVB, *IVR/EVR registratie*, available via this link.

(462) De Vries and Mourcous 2019, pp. 248-249.

(463) The system is managed for insurers by the Dutch Central Information System Foundation (*Stichting Centraal Informatie Systeem*; CIS) and for banks by the Dutch Credit Registration Office (*Stichting Bureau Krediet Registratie*; BKR).

B. Initiatives in the Netherlands and abroad

Protocol on the Incident Warning System for Financial Institutions (PIFI)

IFI participants recognize that inclusion in a (shared) register for fraud, money laundering or forgery has a profound impact on the natural person or legal entity involved. The IFI is therefore regulated by the Protocol on the Incident Warning System for Financial Institutions 2021 (PIFI). The PIFI identifies the role of financial institutions in the prevention of misuse and fraud and emphasizes the importance of cooperation - and by extension the possibility of exchanging information - to prevent misuse and fraud.(464) Given that inclusion in a register constitutes an invasion of the privacy of the natural person or legal entity in question, strict registration criteria apply based on tight proportionality and subsidiarity requirements. The Dutch DPA has approved this protocol and issued a license for the processing of criminal data in accordance with the protocol.(465) The Dutch DPA also supervises compliance with the protocol.

The PIFI sets out conditions for the exchange of data and safeguards against unauthorized use of the data exchange system, including confidentiality and retention periods (Chapter 3 PIFI). For example, section 3.3 PIFI regulates the verification process: in principle, an institution to which a request about a natural person or legal entity is addressed gives a hit/no hit response to the requesting institution. In principle, it is only if there is a hit that the Security Departments of the questioned institution and the requesting institution exchange information about the registration. The Security Department of the requesting institution then advises the employee who made the request. This advice may be for the institution to enter into the relationship subject to conditions, not to enter into it, or to terminate it. It is mandatory for the requesting institution to take this advice into account in its decision-making with regard to the natural person or legal entity in question.(466)

The PIFI also includes requirements regarding access to the registers and indexes, retention periods and deletion of data from the registers and indexes (Chapters 4 and 5). In terms of governance, an advisory committee has been established pursuant to the PIFI. It advises on a range of issues including the application of the reporting criteria, the eligibility and suitability of banks and insurers wishing to join the warning system and the exclusion of participants who do not comply with the protocol (Chapters 6 and 7). The PIFI also contains other rights and obligations of participating financial institutions, such as the obligation of reciprocity or the drafting of work instructions for staff (Chapter 8). Finally, it also stipulates the rights and obligations of natural persons and legal entities who are to be listed in incident registers/the external reference index. In principle, they have the right to be informed about their inclusion and to ascertain whether the register or index includes their personal data. They also have the right to access their data on request. If the data is incorrect, the data subject has the right to have it corrected. Data subjects also have the right to object to the inclusion in the register/index and to be heard by a dispute resolution committee (Chapter 10). Finally, it is important to note that inclusion in an IVR/EVR does not mean that the person or entity in question may be excluded from basic products, such as a basic bank account or basic insurance.(467)

(464) Protocol on the Incident Warning System for Financial Institutions 2021, pp. 6-7. (PIFI 2021).
(465) PIFI 2021, p. 5; Dutch DPA, *Besluit inzake de vergunningaanvraag voor de verwerking van [PARTIJ] volgens het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021*, August 20, 2021, reference z2021-03355, available via this link. Parties that join the IFI later are required to apply for a separate license from the Dutch DPA; see De Vries and Mourcous 2019, p. 250.
(466) Section 3.3.1 PIFI 2021.
(467) PIFI 2021, p. 8.

B. Initiatives in the Netherlands and abroad

2. The development and use of digital identities and authentication tools

2.1. Australia Post Digital iD

According to some of the literature, Australia has "*the most modern form of digital identification*."[468] At the same time, it is also said that the use of national identity systems for multiple purposes in Australia has a "*poor track record*".[469]

Australia's Trusted Digital Identity Framework (TDIF) is a (temporary) accreditation framework for digital identity services which allows both government and private parties to develop and offer digital identities.[470] Although still in a pilot phase, the framework is about to be embedded in law as a result of the 2023 Digital Identity draft legislation.[471] The Australia Post Digital iD has been accredited under this scheme since May 17, 2019; a number of other (commercial) service providers have been admitted since then. The Australia Post Digital iD is considered as the more commercial counterpart to the government-developed GovPass.[472]

It is a commercial service provided by Australia Post, a fully state-owned company. However, the company receives no state funding and actually operates as a commercial company that pays dividends to the government every year.[473] The Australia Post Digital iD is optional for natural persons and works through an app. The user downloads the app, fills out some personal data and takes a selfie. This data is then compared with data from government records. The user must subsequently go to a branch of Australia Post and identify themselves physically by means of a passport or driver's license and the phone on which the app is installed. Their digital identity is then activated[474] and the user can then prove the identity using the app. Parties request the user's consent to retrieve their digital identity, which the user confirms via the app. The data included in Australia Post's Digital iD is limited to the standard data needed to identify individuals and to verify their identity. This includes name, date and place of birth, and place of residence.

One service linked to the Digital iD is Keypass, which enables users to prove that they are over 18 in order to purchase alcohol without sharing their personal data.[475] As of 2021, the Digital iD can be linked to DocuSign, which can be used to digitally sign documents.[476]

Digital identities are not yet (widely) used by Australian institutions as part of their customer due diligence, even though the use of electronic data for identification and verification purposes is allowed.[477] Australia Post Digital iD is, however, offered as a tool for the identification and verification of natural persons when they enter into (and for the duration of) business relationships. According to Australia Post, as part of its AML/KYC service the Digital iD makes it possible to perform other functions such as PEP and sanctions screening.[478]

(468) Rainey et al. 2019, p. 37: *"Australia has the most modern form of digital identification."*
(469) ASPI 2018, p. 3.
(470) See ASPI 2022, pp. 4-5 for a more detailed explanation of the TDIF.
(471) *Digital Identity System: Legislation*, available via this link.
(472) ASPI 2018, p. 7.
(473) Australia Post 2021, p. 4.
(474) Australia Post, *Digital ID*, available via this link; Rainey et al. 2019, p. 37.
(475) Australia Post, *Digital ID*, available via this link.
(476) Australia Post, 'AusPost's Digital iD linked with DocuSign for e-signatures', press release March 24, 2021.
(477) AUSTRAC, *Reliable and independent documentation and electronic data*, available via thislink.
(478) Australia Post, AML solutions: Digital iD AML/KYC offering, available via this link.

B. Initiatives in the Netherlands and abroad

2.2. Singapore Personal Access: Singpass

Singapore's financial regulator Monetary Authority of Singapore (MAS) together with the Smart Nation and Digital Government Office (SNDGO) and the Government Technology Agency (GovTech) have contributed to the development of Singapore's national digital ID: Singapore Personal Access, known as 'Singpass'.(479) Singpass is used by government agencies and (financial) institutions and it is for both natural persons and legal entities. It is available via an app.

Various services can be provided through Singpass:

- *MyInfo* (personal information for KYC purposes)
- *Verify* (verification of customers in a physical situation)
- *Login* (access to digital services)
- *Sign* (digital signing of documents)
- *Biometrics-as-a-service* (biometrics-as-a-service)
- *SafeEntry* (checking in and out of organizations)
- *SGFinDex* (consolidation of financial data)
- *Remote Authorization* for transactions will be added in the future.(480)

These services are linked to the Singpass system via APIs. The government uses the Singpass API portal website to disclose all source information about the architecture, operation of the API and conditions of use to the general public.(481) The following services are used by financial institutions: MyInfo, Sign and SGFinDex.(482)

Use of Singpass services that the government makes entirely available through GovTech is not considered a form of outsourcing according to the financial regulator, the MAS.(483) Financial institutions may therefore use these services and tools without having to comply with additional outsourcing requirements. The reason is that the government already controls the services and society at large is able to use them. We explain the three services in question in more detail below:

1. MyInfo and MyInfo Business

Private individuals use a tool called MyInfo to grant consent for the use of their personal or business data. The tool used by legal entities for this is MyInfo Business. Logging in with Singpass, customers use MyInfo for various purposes such as going through the KYC process of opening bank accounts and applying for credit cards and loans.(484)

Financial institutions are authorized to use this information for their KYC process: MAS accepts MyInfo as an independent and reliable source for the following data: customer name, national ID number, date of birth, nationality and residential address. Financial institutions do not need to perform additional identification or verification or request any form of documentation, or even a photograph of the customer.(485) MyInfo compiles this information from public records: this ranges from personal information (e.g. full name, Tax Identification Number, gender, date of birth, nationality, passport number) to financial information, information about occupation and education, family composition, cars and driver's license, housing, and government programs (e.g. state retirement benefits).(486)

(479) Monetary Authority of Singapore, *Digital ID and e-KYC*, available via this link.
(480) Singpass, *Transforming Singapore through technology*, available via this link.
(481) Singpass, *Transforming Singapore through technology*, available via this link.
(482) Monetary Authority of Singapore, *Digital ID and e-KYC*, available via this link.
(483) Monetary Authority of Singapore, *Circular ID 26/20: Outsourcing arrangements involving services wholly provided by the Government Technology Agency ("GovTech") or agents appointed by GovTech*, June 9, 2020, available via this link.
(484) Singpass, *Singpass API Products*, available via this link; Monetary Authority of Singapore, *Circular ID 26/20: Outsourcing arrangements involving services wholly provided by the Government Technology Agency ("GovTech") or agents appointed by GovTech*, June 9, 2020, available via this link.
(485) Monetary Authority of Singapore, *Circular AMLD 01/2018: Use of MyInfo and CDD Measures for Non Face-to-Face Business Relations*, January 8, 2018, available via this link.
(486) Singpass, *MyInfo: speed up eKYC processes for individual users with data from government sources*, available via this link.

B. Initiatives in the Netherlands and abroad

MyInfo contains over 100 different data points.[487] The goal is to open up all financial institutions to this database and to enable them to modify or update information in order to avoid repeating queries to customers and enhance data quality.[488]

Given its operation, the MyInfo tool in the Singpass system acts as a kind of KYC utility. The difference with the initiatives listed in section 1 of this annex is that MyInfo is developed and managed by the government.

2. Sign

Using Singpass, natural persons and legal entities can use a tool called 'Sign' to digitally sign documents and agreements.

3. SGFinDex

With their Singpass, natural persons can also use the SGFinDex (Singapore Financial Data Exchange) tool to retrieve all their financial data from banks, insurers, central securities depositories and relevant government agencies (to access tax and pension information, for example).

SGFinDex is the product of collaboration between MAS and Smart Nation and Digital Government Group (SNDGO), with support from the Singapore Ministry of Manpower. The tool was built on Singpass by government parties, in collaboration with Singapore's banking and life insurance industry associations and participating financial institutions.

With the data subject's consent, SGFinDex can be used to share and consolidate financial information. This consent is effective for one year.[489]

2.3. Digital identity (e-ID) in Europe and current commercial solutions in the Netherlands

In the EU, the 2014 eIDAS Regulation provides the current basis for unified EU policy on digital identity.[490] The regulation sets requirements for electronic identification and authentication tools, such as electronic signatures. For example, Article 8 of the regulation contains three assurance levels (low, substantial, high) for electronic identification. The level required varies according to the service: the more sensitive the information, the higher the assurance level and the higher the requirements.[491] The regulation also establishes cross-border recognition of government authorities' e-IDs and provides for European citizens and companies to be able to log in to government agencies such as municipalities, provinces and central government using a European-recognized national login means. For authentication tools, also called trust services, a distinction is made between qualified trust services and non-qualified trust services. Qualified trust services are subject to heightened requirements and oversight. In the Netherlands, this is done by the Dutch Authority for Digital Infrastructure (*Rijksinspectie Digitale Infrastructuur*, RDI).[492]

(487) FATF 2020, p. 76.
(488) JFSC 2020, p. 20.
(489) Monetary Authority of Singapore, *Singapore Financial Data Exchange (SGFinDex)*, available via this link.
(490) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *OJEU* L 257, pp. 73-11.
(491) Commission Implementing Regulation 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, *OJEU* L 253, p. 7 (eIDAS Implementing Regulation) sets out the requirements for each assurance level for the various authentication tools.
(492) Dutch Authority for Digital Infrastructure, *Elektronische vertrouwensdiensten*, available via this link.

B. Initiatives in the Netherlands and abroad

In 2020, the European Commission published its strategy for the EU's digital future and introduced "*A Europe fit for the digital age*" as one of its policy priorities.(493) Whitin this plan, the Commission committed to revise the eIDAS Regulation "*to improve its effectiveness, extend its application to the private sector and promote trusted digital identities for all EU citizens and businesses.*"(494)

In June 2021, the European Commission published its evaluation of the operation of the eIDAS Regulation. One of its findings was that eIDAS has limited coverage because only a limited number of e-IDs had been notified and made accessible by Member States. In addition, costs had proven to exceed benefits and there were practical difficulties in recognizing e-IDs.(495) Also, the regulation did not meet market needs: the evaluation found that the most added value was seen in the use of e-IDs in the private sector.(496)

Based on that evaluation and in line with the aforementioned policy priority, the European Commission submitted a proposal for the amendment of the eIDAS Regulation (eIDAS2 Regulation).(497) The main change is the move from a framework for digital identities within different Member States to a single overarching framework for a European digital identity. Specifically, the European Commission proposes that every European citizen and company should have their own European digital ID wallet containing information about identity and, optionally, other data as well, such as diplomas, medical data and powers of attorney (authorizations to act on behalf of legal entities).(498) According to the proposal, natural persons and legal entities will themselves manage their digital identity using an app; for natural persons, the EU digital identity wallet will be free of charge (Article 6a(6) of the eIDAS2 Regulation). They can choose which personal data and documents they want to share, online and offline, with which government agencies and private parties. This will then put the individual in question in control of their data sharing. The regulation provides that EU digital identity wallets must ensure the highest level of security for the personal data used for authentication (Article 6a(6) of the eIDAS2 Regulation). Private parties from a wide range of sectors (transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications) will be required to ensure European digital identity (Article 12b of the eIDAS2 Regulation). Another important change is the extended scope of the eDIAS2 Regulation to other trust services "*to respond to the dynamics of the markets and to technological developments.*"(499) New services that will be included in the scope in the proposal are the management of remote electronic signature and seal creation devices, the provision of electronic archiving services, the provision of electronic ledgers and electronic attestation of attributes, i.e. electronically certified diplomas, for example.(500)

(493) European Commission, *The European Commission's priorities*, available via this link.
(494) European Commission 2021, p. 7.
(495) European Commission 2021, pp. 3-5.
(496) European Commission 2021, p. 8.
(497) Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021) 281 final, 2021/0136(COD), June 3, 2021.
(498) European Commission, *European Digital Identity*, available via this link. See also: DNB 2022, pp. 29-30.
(499) Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021) 281 final, 2021/0136(COD), June 3, 2021, p. 1 (reasons for and objectives of the proposal).
(500) Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021) 281 final, 2021/0136(COD), June 3, 2021, p. 15.

B. Initiatives in the Netherlands and abroad

The Netherlands

In addition to the directly applicable eIDAS Regulation and its successor, eIDAS2, the Digital Government Act *(Wet digitale overheid*; Wdo) was also approved in the Netherlands in March 2023.(501) This Act lays the further foundation for digitization of the government, but also deals with the possibility for citizens and companies to use recognized private login means in addition to DigiD.(502) With regard to the use of digital identities, the Wwft, as indicated earlier in this chapter, allows gatekeepers to use electronic means of identification to establish and verify the identity of customers during customer due diligence, provided they meet a substantial or high assurance level. These may be private electronic means of identification. In a Q&A, the Dutch Central Bank (DNB) states that institutions themselves remain responsible for complying with this requirement and that they must make their own determination that an e-ID tool is sufficiently reliable, or have an expert do so.(503)

Specifically of interest to the notarial profession is the legislative bill on the digital incorporation of private companies with limited liability that was introduced in 2022. This bill seeks to allow the incorporation of a private limited company without the applicant being physically present. Where there is no suspicion of identity fraud or doubt about the applicant's legal capacity, an appearance before a civil-law notary via a video link would be sufficient, with the civil-law notary being able to establish the applicant's identity using an electronic means of identification with a high eIDAS assurance level.(504) The electronic notarial deed can then be signed digitally using an electronic signature.(505) The Royal Dutch Association of Civil-law Notaries (*Koninklijke Nederlandse Beroepsorganisatie*; KNB) is currently developing a tool called NotarisID, partly to enable the digital incorporation of private companies with limited liability. This is a combination of an electronic means of identification with a high eIDAS assurance level and a qualified electronic signature in accordance with the eIDAS Regulation.(506)

There are also several other private and commercial initiatives in the Netherlands that offer digital identity, authentication tools and digital records management services. One example of a digital identity is iDIN: "*a service provided by the banks that allows consumers to access other organizations using the secure and trusted logins of their own bank: identify, log in and confirm age.*"(507) Data that iDIN uses are initials, surname, date of birth, age verification (18+), residential address, gender, email address and/or phone number. This data has been verified by the customer's bank. Customers determine whether and which information may be shared.(508) Another example is Yivi (formerly IRMA). Like the plans for the European ID wallet, Yivi works through an app on a mobile device. Information that can be entered into the Yivi app is personal data such as name, address and contact information. It can also include other attributes, however, such as financial data, diplomas and medical data. The person in question can decide what information to share and with whom.(509) A third example is a service that was Belgian called 'itsme®'. This digital identity also works through an app. To create a digital identity, a mobile device scans the person's ID card or passport. The person is then asked to show him/herself using the phone's camera.

(501) Government of the Netherlands, 'Eerste Kamer neemt Wet digitale overheid aan', news release March 21, 2023.
(502) Government of the Netherlands, *Digital Government*, available via this link.
(503) DNB, *Q&A Electronic means of identification and client identification*, available via this link.
(504) See the proposal for Section 53g in the legislative bill for the Digital Incorporation of Private Companies with Limited Liability Act (*Wet online oprichting besloten vennootschappen*), Parliamentary Papers II, 2021/2022, 36 085, no. 2.
(505) See the proposal for Section 53e in the legislative bill for the Digital Incorporation of Private Companies with Limited Liability Act, Parliamentary Papers II, 2021/2022, 36 085, no. 2.
(506) Information compiled by KPMG based on discussions with the KNB as well as on the KNB website, available via this link.
(507) Currence, *Collective payment products: IDIN*, available via this link.
(508) iDIN, *iDIN - Een veilig iD*, available via this link.
(509) Information compiled, translated and summarized by KPMG from the website: https://www.yivi.app/.

B. Initiatives in the Netherlands and abroad

The person is compared to the photo in their passport using facial recognition. Individuals can use itsme® to identify themselves, authenticate, confirm actions and sign documents digitally.(510) Finally, there are already commercial providers of digital records management or so-called 'digital data vaults', often combined with the provision of a digital signature.(511)

3. Public-private partnerships in the Netherlands

3.1. Fintell Alliance NL

Formally established on the basis of an Alliance document in February 2021, Fintell Alliance NL is a public-private partnership between FIU-NL and the banks ABN AMRO Bank, ING Bank, Rabobank, de Volksbank, Triodos and Knab.(512)

Fintell Alliance NL's objective is for the participating banks to share knowledge and operational intelligence in order to better map criminal networks.(513) By sharing red flags, *modus operandi* and feedback on reports by FIU-NL, the banks in the alliance aim to increase the quality of reports to FIU-NL and criminal investigation services and to improve insights into trends and phenomena in money laundering and terrorist financing.(514) What distinguishes Fintell Alliance NL from other PPP efforts is that it joint content analyses are conducted, to the extent permitted by law. Specifically, analysts and investigators from the banks and FIU-NL meet at a physical location and collaborate on anonymized analyses on a case-by-case basis.

The outcomes of Fintell Alliance's work in this regard are also being used in other PPP contexts, including several FEC task forces and projects (refer to section 3.2 of this annex).(515)

This intensive collaboration between the banks and FIU-NL means that the lines of communication are short. FIU-NL explains the successes of Fintell Alliance NL in its 2021 Annual Review: "*The participating bank analysts made it known that the continuous feedback loop from FIU-the Netherlands was very much worth further developing and refining. The same applies to the FIU analysts, who are making great strides in their knowledge of the financial system, enabling them to interpret unusual transactions even better. This has already resulted in thousands of transactions being declared suspicious and many intelligence reports being prepared on subjects including facilitators, underground banking and criminal networks setting up businesses for drug smuggling. That is concrete financial intelligence for our investigative partners. At the same time, it also leads to more knowledge being shared within the banks, creating a self-reinforcing feedback loop. This enhances the effectiveness of the gatekeeper function of banks in preventing the use of the financial system for money laundering and terrorist financing.*"(516)

3.2. Financial Expertise Center

The Financial Expertise Center (FEC) is primarily a public partnership between authorities with supervisory, monitoring, prosecution or investigative tasks in the financial sector.(517)

(510) Information compiled, translated and summarized by KPMG from the website: https://www.itsme-id.com/nl-NL.
(511) A random selection of examples are Doccle, Vidua, Pondres, the Dutch 'Notarial Vault' (*Nederlandse Notariskluis*), and the 'Digizeker data vault' (*Digizeker datakluis*). KPMG has not assessed their design, operation and existence.
(512) Prior to formalizing the project, FIU-NL and de Volksbank collaborated on a successful pilot project: FIU 2021, p. 4.
(513) FIU 2021, p. 16.
(514) FATF 2022b, p. 59; Financial Intelligence Unit-Netherlands, *Cooperation at the national level*, available via this link; Financial Intelligence Unit-Netherlands, 'FIU-Nederland treedt samen met grootbanken op tegen witwassen en terrorismefinanciering', press release November 2, 2021; NVB, 'Nieuwe publiek-private samenwerking in Fintell Alliance - "Nieuwe boost voor aanpak witwassen"', press release February 11, 2021.
(515) FATF 2022b, p. 59.
(516) FIU 2021, p. 16.
(517) These include the AFM, the Dutch Tax Administration, DNB, FIU-NL, FIOD, the Public Prosecution Service and the police. See Article 1 of the FEC Covenant 2014 (*Staatscourant* 2014, 2351).

B. Initiatives in the Netherlands and abroad

The FEC was established in 1998 in the wake of public interest in an ethical financial sector and the importance of adequate regulation of the financial sector as well as proper administrative and criminal law enforcement in the financial sector.[518] The public partners in the FEC collaborate among themselves as well as with private parties in various programs and projects. This public-private partnership is integrated into the three core tasks of the FEC. These tasks are described and explained below.

1. Creation of a systematic exchange of information between partners

The first core task of the FEC is to facilitate a structural exchange of information.[519] The FEC's primary means of fulfilling this task is the 'FEC Information Platform', which exchanges alerts about potential and actual integrity issues involving individuals or companies.[520] This exchange can help to consolidate the information position of the FEC partners and enable joint interventions where necessary.[521] In the FEC Terrorist Financing Program, the seven FEC partners exchange information among themselves and also with six other public organizations.[522] One of the objectives of this program is, on the basis of alerts, to identify financial networks that may have a relationship with terrorism. Moreover, the FEC partners also develop typologies of potential forms of terrorist financing based on the knowledge gained.[523]

In addition to the information exchanged among the FEC partners themselves, the partners also have task forces for the exchange of information with a group of participating private parties. This is also specifically referred to as the 'FEC PPP'.

There are currently public-private partnerships within the Serious Crime Task Force (SCTF) and the Terrorist Financing Task Force (TFTF).

SCTF

The SCTF began as a pilot in 2019 and was made a permanent, structural part of the public-private partnership in the FEC in 2021. This task force is based on a covenant and a decree pursuant to Section 20 of the Police Data Act (Wpg), which has been approved by the relevant ministries.[524] Within the SCTF, the police, the Public Prosecution Service, FIU-NL and FIOD collaborate with ABN AMRO Bank, ING Bank, Rabobank, de Volksbank, Knab[525] and Triodos[526].

In coordination with the Public Prosecution Service, the police and FIOD also share with FIU-NL names of advisors or legal entities (intermediaries) that, although suspected of possible involvement in organized crime, have not been subject to criminal investigation. The banks and FIU-NL then analyze any information that could potentially result in unusual transaction reports. If FIU-NL declares any unusual transactions suspicious, such information can be made available to the criminal investigation services. The police and FIOD can decide to launch a criminal investigation on that basis.[527]

According to the participants, several successes have already been achieved, "*such as modifying procedures in banks, criminal cases and hundreds of suspicious transactions.*"[528] According to the Public Prosecution Service, in 2022 this involved "*several investigations with more than 700 suspicious transactions, but also the tightening of procedures in banking [...].*"[529]

(518) Decree establishing the financial expertise center of December 31, 1998 (*Staatscourant* 1999, 32).
(519) Article 3 of the FEC Covenant 2014 (*Staatscourant* 2014, 2351).
(520) FEC 2022, p. 20.
(521) FEC 2022, p. 20; FEC 2021, p. 6.
(522) The organizations concerned are Customs, the Royal Netherlands Marechaussee, the Immigration and Naturalization Service, the Financial Supervision Office, the Ministry of the Interior and Kingdom Relations, and the Tax Administration's Allowances Division, see FEC 2022, p. 5.
(523) FEC 2022a, p. 13; FATF 2022b, p. 98.
(524) Serious Crime Taskforce Pilot Covenant, *Staatscourant* 2019, 43629; Police, 'Serious Crime Taskforce leidt tot structurele samenwerking', press release October 25, 2021; FEC, *Taskforces*, available via this link.
(525) Addendum to the Serious Crime Taskforce Pilot Covenant: accession of Knab, *Staatscourant* 2021, 25818.
(526) Addendum to the Serious Crime Taskforce Pilot Covenant: accession of Triodos, *Staatscourant* 2022, 22003.
(527) Police, 'Serious Crime Taskforce leidt tot structurele samenwerking', press release October 25, 2021; FEC, *Taskforces*, available via this link.
(528) Police, 'Serious Crime Taskforce leidt tot structurele samenwerking', press release October 25, 2021.
(529) Public Prosecution Service 2022, p. 18.

B. Initiatives in the Netherlands and abroad

TFTF

The TFTF was set up as a pilot in 2017 and was made a permanent, structural part of the public-private partnership in the FEC in 2019. It is based on the Terrorist Financing Task Force Covenant.(530) Its purpose is "*to enable collaboration between public-sector and private-sector parties aimed at the prevention and criminal prosecution of terrorist financing.*"(531) The police, Public Prosecution Service, FIU-NL and FIOD collaborate with Aegon, ABN AMRO Bank, ING, Rabobank, de Volksbank and Triodos in the TFTF.

The TFTF's *modus operandi* is similar to that of the SCTF, described above. In the TFTF, criminal investigation services share the names of natural persons and legal entities linked to terrorism and its financing with private parties at an early stage. The TFTF's focus is therefore on specific alerts to terrorist financing, while the SCTF is more concerned with transactions that have the potential to expose criminal networks or financial *modi operandi* linked to the advisor or legal entity in question.

2. Creation of a knowledge center by and for parties working in areas relevant to the FEC

The FEC's second core task is the creation of a knowledge sharing center.(532) It shares knowledge as follows: for example, between mutual contacts, collaboration between the FEC partners, knowledge meetings ('FECademies') or within and among the FEC's various bodies and platforms (e.g. the FEC privacy platform).

Besides public parties sharing knowledge among themselves, knowledge is also shared between private and public parties in the FEC PPP Expert Platform.(533) The FEC also maintains contacts with foreign organizations and takes part in international knowledge sharing meetings.(534)

3. Implementation of projects aimed at obtaining concrete, operationally useful results

The third core task of the FEC is the joint implementation of projects in various themes and/or phenomena, both among the authorities and in public-private partnerships.(535) Recent projects have included cryptocurrencies, the synthetic drug industry and illegal trust services.(536) These projects are aimed at sharing and increasing insights, knowledge and skills.(537) Unlike in the case of task forces, no personal data is exchanged in these projects. Whereas the task forces currently only collaborate with the banking sector, a project on cryptocurrencies in 2022 also involved collaboration with crypto service providers.

3.3. AMLC

The Anti-Money Laundering Center (AMLC) was established in 2013 on the initiative of the Fiscal Intelligence and Investigation Service (FIOD) and is also part of this organization. The AMLC is a knowledge and expertise center where public and private parties work together nationally and internationally in the fight against money laundering and terrorist financing.(538)

(530) Terrorist Financing Task Force Covenant, *Staatscourant* 2019, 43628.
(531) FEC, *Taskforces*, available via this link.
(532) Article 3 of the FEC Covenant 2014 (*Staatscourant* 2014, 2351).
(533) FEC 2022, p. 17. The participating private parties are ABN AMRO, ING Bank, Rabobank, de Volksbank and the NVB.
(534) FEC 2022, pp. 23-25.
(535) Article 3 of the FEC Covenant 2014 (*Staatscourant* 2014, 2351); FEC 2022, p. 6.
(536) For more information, including on other projects, see FEC 2022, pp. 6-16. Specifically on the project targeting illegal trust services, see also FATF 2022b, pp. 148-149, where the FATF describes the problem of trust service providers (some of them formerly licensed) attempting to circumvent DNB supervision by splitting up their services; also described is this project's approach to tackling the problem.
(537) FEC 2022, p. 6.
(538) AMLC, *Who we are and what we do*, available via this link. See also: Diepenmaat 2021, p. 126.

B. Initiatives in the Netherlands and abroad

Public parties to the AMLC include the Public Prosecution Office, FIU-NL, the Royal Netherlands Marechaussee, RIEC-LIEC, various regulators and special criminal investigation services. Private-sector parties that the AMLC collaborates with include banks, civil-law notaries and audit firms.(539)

Knowledge development and sharing

As a knowledge and expertise center, the AMLC endeavors to increase knowledge about money laundering and terrorist financing on the basis of data and information. It generally works on specific projects or addresses particular themes.(540) Examples include formulating and reformulating money laundering typologies, identifying new phenomena and developing new reporting indicators.(541) On its website, the AMLC publishes case law, in-depth articles, literature and resources related to the strategic themes. The AMLC also regularly broadcasts podcasts in which AMLC experts and guests (from both the public and private sectors as well as academia) elaborate on certain money laundering topics. In addition, it develops training materials for both its public and private partners.(542)

Support for criminal investigations

In addition to this active role in developing and sharing knowledge with a wide audience, the AMLC supports FIOD and other public partners carrying out criminal investigations. Although the AMLC does not conduct such investigations itself, it is able to assess and enrich alerts submitted to it.(543) As part of FIOD, the AMLC has access to criminal investigation information from various sources as well as the FIU unusual transaction reports database. The FATF evaluation of the Netherlands commends its "*unique data availability*" and cites the 'AMLC Suite' as an example of a data hub. The AMLC Suite is a browser that allows authorized criminal investigators to search combined information across multiple sources, e.g. FIU reports, police and criminal records, and information from public sources (such as various Leaks and Papers).(544)

3.4. National and Regional Information and Expertise Centers (LIEC/RIEC)

The National Information and Expertise Center (LIEC) and the ten Regional Information and Expertise Centers (RIECs) are collaborative bodies established since 2008 that provide a broad range of support to the government partners in the fight against organized and subversive crime.(545) The RIEC-LIEC system does this by raising awareness of the problem of organized and subversive crime among government and private-sector parties, supporting and strengthening collaboration both within government and with private parties, and sharing knowledge and expertise on an administrative and integrated approach to subversive crime.

(539) AMLC, *Who we are and what we do*, available via this link; FATF 2022b, p. 60.
(540) The current strategic themes of the AMLC are financial safety, trade-based money laundering and concealed assets. See: www.amlc.nl.
(541) AMLC, *Wat wil het AMLC bereiken*, available via this link. See also FATF 2022b, p. 41; Diepenmaat 2021, p. 126.
(542) FATF 2022b, p. 43.
(543) ECORYS 2018, p. 155.
(544) FATF 2022b, pp. 41 and 51.
(545) Article 2 of the Covenant on the Administrative and Integrated Approach to Organized Crime, Combating Enforcement Bottlenecks and Promoting Integrity Assessments (the "RIEC-LIEC Covenant"); RIEC-LIEC 2021, p. 8. The following government agencies are signatories to the RIEC-LIEC Covenant: Municipalities, Provinces, the Tax Administration, FIOD, Customs, the Netherlands Labor Authority, Police, Royal Netherlands Marechaussee, Public Prosecution Service, Immigration and Naturalization Service, Employee Insurance Agency, and the Netherlands Food and Consumer Product Safety Authority.

B. Initiatives in the Netherlands and abroad

The RIEC-LIEC's focus is both regional and national as well as international. The regional work done by the RIECs is based on the idea that organized subversive crime usually originates and is anchored in the country's regions.(546) The LIEC supports the RIECs where tasks affect all the RIECs but are too costly or specialized to be entrusted to each of them.(547) The LIEC also shares best practices and experiences with the RIECs.(548) Internationally, the LIEC-RIEC collaborates with Belgium and Germany in EURIEC.(549)

The RIEC-LIEC addresses a number of themes in the fight against organized and subversive crime, one of which is money laundering and related forms of financial and economic crime. Other themes include human trafficking and smuggling and organized hemp cultivation.(550) In 2021, most RIEC cases dealt with money laundering.(551)

Collaboration with the private sector

Companies that can be used as facilitators of criminal activities are the main target in the RIEC-LIEC's collaboration with private-sector parties. Examples of such parties are gatekeepers, but also schools, airports, ports or the Royal FloraHolland auction. The public-private partnership is not primarily aimed at investigating and prosecuting criminals, "*but rather at preventing and/or disrupting subversive crime on the one hand and building structured and enduring partnerships on the other.*"(552)

The RIEC-LIEC's public and private partners aim to share knowledge and expertise. Activities undertaken in this regard include organizing awareness meetings and meetings with parties in the sectors in question. At the national level, the LIEC organizes what are called 'national phenomenon tables'. The first of these dealt with subversive crime in the real estate sector. Civil-law notaries and real estate agent-appraisers are relevant private-sector parties in the RIEC-LIEC's PPP context.

The RIEC-LIEC also has PPPs that tackle joint projects. Projects initiated under PPPs are aimed at preventing and disrupting crime as well as building structured and enduring partnerships. Some examples of money laundering projects include:

- an investigation commissioned by RIEC Amsterdam-Amstelland together with the Amsterdam Real Estate Agents Association (*Makelaarsvereniging Amsterdam*) regarding the extent to which Amsterdam real estate agents create barriers to criminal activity by exercising their gatekeeper function;(553)
- a study called 'Money laundering with real estate' (*Witwassen via vastgoed*), which has been commissioned by RIEC The Hague. Its purpose is to teach municipalities to recognize and prevent money laundering through real estate, and to find out which signatories to the RIEC covenant or private partners are needed in this regard;(554)
- the 'civil-law notary' project, aimed at countering the laundering of criminal funds, conducted by RIEC Noord-Nederland.(555)

(546) Article 3 of the RIEC-LIEC Covenant; RIEC-LIEC 2021, p. 8.
(547) Article 4 of the RIEC-LIEC Covenant; RIEC-LIEC 2021, p. 8.
(548) RIEC-LIEC 2021, p. 29.
(549) For more information, see this link.
(550) Article 2 of the RIEC-LIEC Covenant; RIEC-LIEC 2021, p. 12.
(551) RIEC-LIEC 2021, p. 15.
(552) RIEC-LIEC 2021, p. 29.
(553) Bureau Broekhuizen 2022.
(554) RIEC The Hague 2022, p. 6.
(555) RIEC-LIEC 2021, p. 29.

B. Initiatives in the Netherlands and abroad

4. Central government steering

4.1. National risk assessments

A comparative study on NRAs in eight countries, including the Netherlands, shows great diversity in design, implementation and reporting.(556) The quality of NRAs appears to be limited, as none of the NRAs studied provide a well-researched and comprehensive risk assessment. Ferwerda and Reuter note that all NRAs have fundamental problems, which they distinguish based on the conceptual framework in question ('conceptual confusion'), the sources of information and methods of analysis used, and the usefulness of the results.(557)

All this makes a deepdive challenging. Nevertheless, our own analysis of various NRAs in other countries provide possible inspiration for an improvement of the NRA in the Netherlands. The deepdive carried out highlights three aspects that may be of interest to the Dutch government in strengthening and deepening the NRA, specifically the methods of analysis applied, sectoral risks and geographic risks.

Methods of analysis

According to the study cited above, the Dutch NRA relies almost entirely on expert opinions: "*[a]t an extreme, the Dutch NRA made use only of expert opinion; it presented no data of any other kind.*"(558) However, the researchers do note that the method of analysis used in the Netherlands can be regarded as the most advanced of all the countries involved in the study.(559) Other sources of information used in other NRAs include reports of unusual (or suspicious) transactions, criminal investigations, statistics, literature and reports.(560) The Italian NRA contains the greatest diversity of information sources.(561)

In the Dutch NRA on Money Laundering, the threat analysis is framed in terms of the money laundering methods employed.(562) Since money laundering is a secondary criminal offense and occurs in the wake of the predicate offenses, a more nuanced risk sketch should be possible. One example of an approach from the perspective of predicate offenses is provided by the U.S. NRA.(563) The Irish NRA also approaches the aspect of threat on the basis of predicate offenses and then links them to commonly used money laundering typologies.(564) The Canadian NRA classifies predicate offenses into different risk groups based on the degree of "*sophistication, capability, scope, and proceeds of crime.*"(565) It is worth considering examining the NRA from the perspective of underlying crime, basic offenses and, by extension, the money laundering methods used in them.

The Dutch NRA analyzes the residual risk of money laundering, i.e. the risk that remains after policy instruments are deployed. The literature suggests that when methods of analysis other than relying (primarily) on expert opinion are applied, assessments of inherent risk could carry more value.(566) Some other NRAs are already turning the focus to inherent risks. The Canadian NRA is one clear example of this; another would appear to be the NRA of the United Kingdom.(567)

(556) Ferwerda and Reuter 2022, pp. 7 and 19.
(557) Ferwerda and Reuter 2022, p. 19.
(558) Ferwerda and Reuter 2022, p. 21.
(559) Ferwerda and Reuter 2022, p. 16.
(560) Ferwerda and Reuter 2022, pp. 15-16.
(561) Ferwerda and Reuter 2022, p. 21.
(562) WODC 2020, p. 46.
(563) U.S. Department of the Treasury 2022a.
(564) Irish Department of Finance 2019, pp. 28-38.
(565) Government of Canada 2023a, p. 17.
(566) Ferwerda and Reuter 2022, p. 36.
(567) UK HM Treasury 2020.

B. Initiatives in the Netherlands and abroad

Sectoral risks

Compared to the Dutch NRA on Money Laundering, foreign NRAs do more to analyze sectoral risks. They do so in different ways. For example, the Belgian Anti-Money Laundering Law requires regulators to conduct their supervision based on risk assessments.(568)

Belgian regulators publish their sectoral risk assessments based on the European Commission's supranational NRA as well as the Belgian NRA, and supplemented by their own regulatory observations and supervision data.(569) This not only means that their risk assessments are the starting point for risk-based supervision, but also allows gatekeepers to be informed of this additional analysis specific to their sectors and services. Similarly, in the United Kingdom, regulators publish sectoral risk assessments in addition to the NRA "*in order to help firms to better estimate the risks they are exposed to.*"(570) The Irish government has published various sectoral or thematic risk analyses in addition to the NRA. Currently, there are four such risk analyses: the gambling sector (2018), new technologies(571) (2019), legal entities and legal arrangements (2020), and trust and company service providers (2022).(572) The German government extensively examines specific risks for the different categories of its gatekeepers in its NRA.(573) It has also published a sectoral risk analysis that addresses the specific vulnerabilities of legal entities and other legal arrangements to money laundering and terrorist financing.(574) The Irish NRA also contains a more detailed account of the specific money laundering threats for each category of gatekeeper.(575)

Finally, the analysis of the degree of vulnerability in the Italian NRA takes a sectoral perspective, through which the relative vulnerability for each category of gatekeeper is determined.(576)

Geographic risks

Some NRAs also address geographic risks to the country, or regional differences in money laundering risks within the country. The German NRA, for example, sets out a comprehensive analysis of potential money laundering risks to the country from a geographical perspective. This includes neighboring countries, countries with substantial German populations and vice versa, countries that Germany has a strong economic relationship with and high-risk countries.(577) The Italian NRA addresses regional differences in terms of cash use, assuming that cash is an indicator of money laundering risks.(578)

4.2. Canada

In March 2023, Canada published its first national strategy entitled 'Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy 2023-2026'.(579) It is based on Canada's National Inherent Risk Assessment and multiple reviews of Canada's anti-money laundering policies. The strategy lists four priorities.

1. Increasing operational effectiveness;
2. Addressing legislative and regulatory gaps.
3. Improving regime governance and coordination.

(568) Section 87 of the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash.
(569) See, for example, College van toezicht op de bedrijfsrevisoren 2023; National Bank of Belgium 2020.
(570) See, for example, UK Solicitors Regulation Authority 2021, pp. 1-2; ICAEW 2022.
(571) This involves looking at cryptocurrencies, crowdfunding and electronic money.
(572) Irish Department of Finance, *National Risk Assessment - Money laundering and Terrorist Financing*, available via this link.
(573) German Federal Ministry of Finance 2019, pp. 55-107.
(574) German Federal Ministry of Finance 2020.
(575) Irish Department of Finance 2019, pp. 39-76.
(576) MEF 2019, pp. 28-31.
(577) German Federal Ministry of Finance 2019, pp. 31-33.
(578) MEF 2019, pp. 8-11.
(579) Government of Canada 2023.

B. Initiatives in the Netherlands and abroad

4. Contributing to international community efforts to combat money laundering and terrorist financing.

Thirteen activities are defined on the basis of the four priorities. These generally involve commitments toward making certain efforts and, to a limited extent, to achieving concrete results or outcomes. The strategy does not include a time schedule, apart from the fact that it covers the years 2023 through 2026.

Public-private partnerships are one of the key focal points of the strategy. The Canadian government underlines the importance of collaboration with the private sector because that allows it to identify potential money laundering and terrorist financing risks, uncover broader financial connections, and provide intelligence to further certain investigations.(580) In terms of improving regime the governance and coordination of its policy Canadian government is, for example, committed to expanding public-private partnerships. The government agencies involved "*will continue to build on these partnerships and work with businesses (…) to improve information-sharing, increase value-added intelligence products, and implement relevant technology to continue to mitigate money laundering and terrorist financing activities.*"(581) The strategy does not specify this any further.

4.3. United States

The United States' strategy to counter money laundering and terrorist financing is set out in its National Strategy for Combating Terrorist and Other Illicit Financing, drafted by the U.S. Department of the Treasury.(582) The most recent version dates from May 2022 and has a two-year term. It is based on the risks identified in national risk assessments of money laundering, terrorist financing and proliferation financing. Published in 2022, the strategy contains four priorities:

1. enhancing transparency and closing legal and regulatory gaps in the U.S. anti-money laundering and combating of terrorist financing regulatory framework;
2. continuing to make the anti-money laundering and combating of terrorist financing regulatory framework for financial institutions more effective and efficient;
3. enhancing the operational effectiveness of combating money laundering, terrorist financing and proliferation financing;
4. enabling the benefits of technological innovations while mitigating risks of money laundering, terrorist financing and proliferation financing.

These four priorities are developed into fourteen supporting actions, with various concrete outcomes identified for each action. These include both hard outcomes and best-efforts obligations.

The strategy places particular emphasis on the risk-based approach, collaboration (including public-private partnerships) and technological innovation. Regarding this risk-based approach, it is worth noting the 2021 FinCEN National AML/CTF Priorities.(583) Based on the previous national strategy, these priorities address the greatest threats to the United States. Institutions are expected to incorporate these priorities into their internal policies. The priorities are geared towards eight predicate offenses for money laundering: corruption, cybercrime (including cryptocurrency), domestic and international terrorist financing, fraud, transnational criminal organization activity, drug trafficking organization activity, human trafficking and human smuggling, and proliferation financing.(584)

(580) Government of Canada 2023, p. 10.
(581) Government of Canada 2023, p. 19.
(582) U.S. Department of the Treasury 2022.
(583) FinCEN stands for 'Financial Crimes Enforcement Network' and is the U.S. counterpart of FIU-NL: FinCEN, 'FinCEN Issues First National AML/CFT Priorities and Accompanying Statements', press release June 30, 2021.
(584) FinCEN 2021, pp. 1-2.

B. Initiatives in the Netherlands and abroad

When publishing its national priorities, FinCEN announced that it would be issuing regulations and guidance on how institutions should incorporate these priorities into their risk-based approaches. However, based on public information, this does not appear to have been followed up yet.

The 2022 strategy does state, however, that national money laundering and terrorist financing priorities are regularly updated and shared with the private sector.(585) For example, as regards technological innovation to promote increased gatekeeper compliance with laws and regulations, the U.S. government expresses a commitment to the development and adoption of digital identity solutions for use by both government and financial institutions. The strategy also includes a consideration of creating a 'regulatory sandbox'.(586)

4.4. United Kingdom

In the United Kingdom, the second Economic Crime Plan 2023-2026 ("ECP2") was published in March 2023.(587) It follows on from the first plan that ran from 2019-2022, which in turn followed on from a 2016 Action Plan for anti-money laundering and counter-terrorist finance, the 2017 Anti-Corruption Strategy and the 2018 Serious and Organised Crime Strategy.(588)

The ECP2 is a joint action plan between the public and private sectors. The private sectors involved are the banking, insurance, accounting, and legal sectors.(589) The Economic Crime Strategic Board, which brings together figures from the public and private sectors, monitors compliance with the plan and progress.

The ECP2 sets three strategic priorities:

1. reducing money laundering and recovering more criminal assets;
2. combating kleptocracy and driving down sanctions evasion;
3. cutting fraud.

The plan also identifies some other themes within each of these selected strategic priorities. The first priority (reducing money laundering) concerns limiting the abuse of British corporate structures; increasing the effectiveness of the regulatory and supervisory regime; combating criminal abuse of cryptoassets; improving intelligence, feedback and analysis through a reform of the reporting system; recovering more criminal assets; furthering the cross-system operational response to money laundering in the light of risks and vulnerabilities. These themes are then developed into concrete actions, along with the organizations responsible for them (both public and private), concrete outcomes and associated outcomes. In total, the plan lists 43 actions.(590)

Recognizing that public-private collaboration is critical, the ECP2 states that "*directing public-private resource towards priority areas will enable us to maximise our collective impact against the threat.*"(591) With the plan the government commits itself to working with the private sector to develop "a clear single version of the truth," with a shared understanding of the risks and vulnerabilities and within which priorities can be set. According to the plan, this involves the government working with the private sector to explore how the former can support the latter in playing its role in a more risk-based manner.(592)

(585) U.S. Department of the Treasury 2022, p. 15.
(586) U.S. Department of the Treasury 2022, p. 25.
(587) UK HM Government 2023.
(588) UK HM Treasury and Home Office 2019.
(589) The organizations involved are: UK Finance, Association of British Insurers, all professional accountancy organizations brought together in the Accountancy AML Supervisors Group (AASG) and The Law Society of England and Wales.
(590) UK HM Government 2023.
(591) UK HM Government 2023, p. 68.
(592) UK HM Government 2023, p. 68.

B. Initiatives in the Netherlands and abroad

Action 33 proceeds from this. This action point focuses on strengthening the role of the National Economic Crime Centre (NECC)[593] as the 'system leader' responsible in collaboration with regulators and the wider public sector for informing priorities and defining a single view of the system to combat economic crime, as well as identifying activity which can be 'de-prioritized' to free up resources for high-utility activity.[594] This action also sets specific quarterly milestones.

The plan recognizes the importance of information sharing, data and technology, noting that information sharing is not optimal at present. There are legal and technological challenges, and where information sharing is possible, the lack of standardization, among other things, plays a limiting role.[595] The ECP2 announces a 'public-private economic crime data strategy' to address this.[596] It also states that the government will continue to engage with industry and civil society regarding the potential for new technology to strengthen efforts to tackle economic crime.[597]

4.5. Italy

The Italian government is commended for its fight against the Mafia. In the Dutch Coalition Agreement 2021-2025 entitled *Looking out for each other, looking ahead to the future*, dated December 15, 2021, the Dutch coalition parties stated their intention to apply the lessons learned from Italy in strengthening the approach to tackling subversive crime.[598] Although particularly relevant from a criminal law perspective, given the integrated Italian anti-Mafia legislation and powers for criminal investigation services and judicial authorities, the preventive anti-money laundering policy is also closely related to this. The FATF notes in this regard that Italian coordination is strong.[599]

Central to this coordination is the *Comitato di Sicurezza Finanziaria* (CSF). Established in 2001[600], this committee operates under the Italian Ministry of Economy and Finance (MEF) and is chaired by the MEF's Director General.[601] In principle, the CSF is composed of representatives from various ministries (i.e. the Interior, Justice, Foreign Affairs and International Cooperation, and Economic Affairs and the MEF itself), the Italian Central Bank, the financial regulators of the capital markets (CONSOB) and insurance sector (IVASS), the Italian FIU, and various criminal investigation services including the Guardia di Finanza, the Carabinieri, various anti-Mafia and terrorism services, and a representative from Italian Customs.[602] The CSF's tasks include the following:[603]

- Coordinating approaches to money laundering and terrorist financing;
- Advising the Ministry of Economy and Finance on the prevention of money laundering and terrorist financing;
- Drafting the NRA;[604]
- Implementing and enforcing international sanctions.

(593) The NECC is a public body established in October 2018 specifically with a view to playing a coordinating role in policies aimed at countering economic crime, including money laundering. The NECC operates under the auspices of the National Crime Agency (NCA), the criminal investigation service responsible for combating serious and organized crime. See: National Crime Agency, *National Economic Crime Centre*, available via this link.
(594) UK HM Government 2023, p. 69: "*Strengthen the role of the NECC as the system leader responsible in collaboration with regulators and wider public sector for informing priorities for the economic crime system and defining a single view of economic crime threats, and in tandem identify and agree activity which can be de-prioritised to enable an increased focus on high-utility activity.*"
(595) UK HM Government 2023, p. 71.
(596) UK HM Government 2023, pp. 72-73.
(597) UK HM Government 2023, p. 71.
(598) See 'Onderzoek: Italiaanse maffia-aanpak deels bruikbaar voor Nederland', *NOS.nl* June 7, 2023. See the University of Groningen 2023 for the full study cited in this article.
(599) University of Groningen 2023; FATF 2016, p. 22.
(600) The committee was originally established by legislative decree 369/2001 dated October 12, 2001. Article 5 of legislative decree 90/2017 dated May 25, 2017 regulates the duties and responsibilities of the CSF. Currently, the composition and functioning of the CSF are laid down in Article 3 of legislative decree 109/2007 dated June 22, 2007; further rules on the functioning of the committee are set by MEF Decree 59/2022 dated April 22, 2022.
(601) MEF 2020, p. 13.
(602) MEF 2020, p 13; FATF 2016, p. 126. The CSF is complemented by the government ownership agency in the context of asset freezing and other sanctions regulations.
(603) MEF 2020, p. 13.
(604) MEF 2019.

B. Initiatives in the Netherlands and abroad

Of particular relevance to this deep dive is the coordinating role of the CSF. Composed of a large and wide-ranging group of government representatives, it shares responsibilities for preventing money laundering and terrorist financing. The committee's members cooperate with each other and exchange information, which includes the authority to override any applicable confidentiality obligations.(605) According to the FATF, "*[d]etailed rules for the exchange of information and collaboration among the agencies concerned are established under article 9 of the AML Law. These agencies are required to cooperate and coordinate, and a Memoranda of Understanding (MOUs) must be signed between them.*"(606)

The CSF is required to report annually to the Minister of Economy and Finance, with a view to the report's submission to Parliament, regarding the efforts made to prevent money laundering and terrorist financing. In these annual reports, the committee sets out proposals for improvements to methods of combating money laundering.(607)

The overarching regulatory framework and the joint responsibility of relevant government parties for coordinating anti-money laundering policy enables these parties to collaborate effectively and efficiently to achieve shared legal objectives.

(605) Information compiled and translated by KPMG from the Italian Ministry of Economy and Finance's website, available via this link. For more information, see FATF 2016, pp. 22 and 149; UIF 2021, p. 128.

(606) FATF 2016, p. 129.

(607) Article 5(7) of legislative decree 90/2017.

List of parties interviewed

C

C. List of parties interviewed

Organizations

In alphabetical order:

1. Autoriteit Financiële Markten (AFM, The Dutch Authority for the Financial Markets)
2. Belastingdienst – Bureau Toezicht Wwft (The Dutch Tax Administration/Wwft Supervision Office)
3. Bureau Financieel Toezicht (BFT, Financial Supervision Office)
4. De Nederlandsche Bank (DNB, the Dutch Central Bank)
5. Financial Intelligence Unit-Netherlands (FIU-NL)
6. Holland Quaestor
7. Koninklijke Notariële Beroepsorganisatie (KNB, The Royal Dutch Association of Civil-law Notaries)
8. Koninklijke Vereniging MKB-Nederland (The Royal Association MKB-Nederland)
9. Nederlandse Vereniging van Banken (NVB, The Dutch Banking Association)
10. The Public Prosecution Service (OM)
11. Vereniging van Makelaars en Taxateurs in onroerende goederen NVM U.A. (NVM)
12. Vereniging VBO - Vereniging van Makelaars & Taxateurs
13. Verbond van Verzekeraars (The Dutch Association of Insurers)
14. VNO-NCW (The Confederation of Netherlands Industry and Employers)

Experts

15. Utrecht University (1)
16. Vrije Universiteit Amsterdam
17. The Offshore Knowledge Centre (*Offshore Kenniscentrum*)
18. Utrecht University (2)

KPMG

This English document represents a translation of the Dutch KPMG report ‘Krachten gebundeld. Naar een effectievere en efficiëntere invulling van de poortwachtersrol in Nederland’. In the event of ambiguities or discrepancies, the Dutch version prevails.

Document classification: KPMG confidential