From recovery to balance

A look ahead to a more risk-based approach to preventing and combating money laundering and terrorist financing

DeNederlandscheBank
EUROSYSTEEM

→

Content

Summary and recommendations

Society must be able to rely on financial institutions to contribute to the prevention and fight against financial crime without unnecessarily burdening their customers or compromising the financial services they offer. There is great societal urgency to actively combat financial crime. Money laundering undermines public confidence in the financial sector. Criminal and terrorist organisations and individuals use laundered money for their own benefit and to finance additional activities. The amount of criminal money earned in the Netherlands is estimated to be EUR 16 billion annually. Ultimately, law-abiding citizens pay the price. They are confronted not only with higher taxes, but also with a society that is less safe and in which the rule of law is undermined. Concurrently, efforts to combat financial crime must not result in generic restrictions on financial services, which can also have an impact on ordinary citizens.

As the supervisory authority, De Nederlandsche Bank ensures that institutions have the necessary procedures and measures in place to prevent and combat financial crime. This report focuses on the role that banks play in combating money laundering and terrorist financing, and our supervision in this regard. Banks play a pivotal role in the financial system. In line with international obligations, Dutch legislation thus assigns banks a key mandate as gatekeepers in preventing and combating money laundering and terrorist financing. In recent years, we, along with the Public Prosecution Service, have found that some institutions in the banking sector have failed to comply fully with applicable legislation. In response, we imposed substantial enforcement measures. The Public Prosecution Service concluded out-of-court settlements with two banks. Partly in response to this, banks have significantly increased their efforts to ensure compliance with the law, but not every bank is equally advanced in this respect. Customer files are being put in order. Banks have tightened their policies on customer acceptance and terminating customer relationships. The number of unusual transactions reported by banks has risen sharply. The range of tools available under administrative law has expanded through the years, providing us with greater support in our work to strengthen the foundation for combating financial crime. We will continue to use all means at our disposal to achieve compliance with the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme - Wwft*) throughout the sector.

A more risk-based approach can enhance the efficiency and effectiveness of preventing and combating financial crime. Boosting effectiveness primarily means that less criminal money will find its way into the financial infrastructure: criminals will be stopped at the gate more frequently. And when criminal money does enter the system, improved detection measures will result in more convictions and confiscations. Boosting efficiency in the fight against financial crime means reducing the administrative burden on banks and their customers. Both more effective and more efficient: it *can* be done. Through a more risk-based approach by banks and supervisory authorities. Through the smarter application of data-driven technological innovations. Through more focused cooperation throughout the chain. These efforts must not be dominated by the fear of making mistakes. Rather, they must engender confidence that working closely together with all parties involved is the best way to prevent and combat financial crime in the Netherlands.

Our research shows that banks are severing relationships with customers in substantial numbers or are not accepting new customers. We conducted a survey among the four largest retail banks in order to gain more insight into the question of how often banks exclude customers from their services (or limit the services they provide) and their reasons for doing so. The survey revealed that these four banks ended their relationship with 7,700 customers in 2021 because of risks related to money laundering or terrorist financing. Banks do not seem to be engaging in categorical exclusion: these customers came from a wide range of economic sectors. Although 7,700 is a substantial number in absolute terms and in view of the repercussions for the customers in question, it represents only 0.02% of the number of private customers and 0.17% of the number of business customers of these four banks. The number of potential customers who were not accepted for the same reason cannot be fully determined on the basis of the survey; a rough estimate places the number at about 7,000.

Both banks and supervisors can adopt a more risk-based approach to preventing and combating money laundering and terrorist financing. The risk-based approach is laid down in international and national frameworks, which serve as important guidelines both for gatekeeper institutions and for supervisors. The challenge for both is to put the risk-based approach more emphatically and more effectively into practice, especially during the recovery phase. First and foremost, this requires improved risk identification. Secondly, the measures taken should be more proportionate to the risks identified: greater risks require stricter measures, while simpler measures are sufficient for smaller risks. This strategy will make it possible to deploy scarce resources where they will be most effective.

Banks can assist their customers by only requesting information that is necessary in view of the potential risk, and by explaining why the information is required. For higher risks, banks need to request more information from customers in order to estimate the risk more accurately and to take the most appropriate control measures. Customers may perceive these requests to be annoying and disproportionate. Customers tend to be willing to help combat money laundering and terrorist financing, which is why banks should clearly explain why specific information is being requested. Sector associations and banks can improve their cooperation in this regard by focusing both on sharper and more specific risk analyses, as well as on the targeted provision of information. Consultations under the aegis of the National Forum on the Payment System provide a framework to this end. While respecting privacy safeguards, it would be beneficial if banks had greater legal scope to consult public registers (municipal personal records database, UBO register). It should also be possible for different institutions to exchange information more extensively (provided the customer gives permission), so that a customer does not have to provide the same information more than once.

We expect banks to adopt a more risk-based approach, both in their recovery operations and systemically. A more risk-based approach can help banks assess customer risks in an appropriate and more balanced manner. Banks should adopt an holistic view for the risk assessment of the individual customer. It is vital that this risk assessment is accurate, for a faulty assessment has consequences that can work both ways. On the one hand, if a bank underestimates risks, it may take too few risk control measures. On the other hand, overestimating risks could cause a bank to take measures that are too numerous and intensive, which could unduly restrict access to banking services and confront the customer with unnecessarily invasive requests for information and documentation. A more risk-based approach can help strike a better balance between risks and measures, while also reducing the number of faulty assessments and limiting unnecessary de-risking. Wherever possible, we issue policy statements that give banks confidence that they are staying within the legal framework when operating according to this approach.

A risk-based approach is at the heart of our supervision of the banks' gatekeeper role when it comes to financial crime. Our supervision is always squarely based on the purpose of the law: ensuring a sound and ethical financial sector. We intend to take the risk-based approach to a higher level in the coming period, both in our supervision and in the risk-based application of relevant legislation by banks. We see a more risk-based approach by banks as an important supervisory focus. This is also the case when monitoring banks' recovery operations. A risk-based approach in our own activities will ensure that we deploy greater supervisory capacity where the risks are greater, and less capacity where they are more limited. Risk analysis is therefore essential for us as a supervisory authority.

We will increasingly emphasise a risk-based approach in our policy communications and documents, and provide scope for innovative solutions. We support institutions by providing guidance on what we expect from them. Wherever possible, we will work with supervised institutions to analyse situations resulting in low or high risk, and investigate how confidence can be both given and obtained that the right measures are being taken for the risks identified. In doing so, we will ensure scope for innovative solutions, especially if they are more effective than traditional approaches. In some cases the law may not formally allow for the application of an innovative solution, even though such a solution may support the purpose of the law. In such cases we nevertheless intend to explore possibilities, for example by engaging with legislators on the removal of dispensable obstacles. Wherever possible, we will use policy statements to address low-risk situations and proportionate control measures.

We provide institutions with scope for experimenting with digital innovations in the fight against financial crime, specifically in the areas of machine learning and digital identity. The use of techniques such as artificial intelligence can improve risk assessments, thus boosting the effectiveness and efficiency of customer due diligence and transaction monitoring. Digital identities can dramatically simplify the identification and verification of customers, for example, leading to a reduction of the administrative burden both for the institution and the customer. A condition for responsible innovation is that the underlying compliance processes are in order pursuant to the *Wwft*, that the IT infrastructure is reliable and that the quality and availability of data are guaranteed. Bias must moreover be avoided. Safeguards must also be in place for privacy and data protection, as well as for the explainability of the models used.

An effective approach to combating money laundering and terrorist financing is only possible if all parties involved work together. The Financial Action Task Force (FATF) has identified the robust system of national cooperation and coordination, both from a policy and operational perspective, as a strength. Nevertheless, the effectiveness of cooperation can be improved. This requires each partner in the chain to operate based on the shared goal of preventing and combating the misuse of the financial system for money laundering or terrorist financing. Concrete and measurable operational objectives and priorities can then be set, so that specific topics and risks can be jointly addressed. The required levels of staffing and other resources must therefore be available. The Financial Expertise Centre plays a coordinating role in this regard.

The process for reporting and investigating unusual transactions can be made more effective. Legislation could be amended, whereby institutions are no longer required to report "unusual" transactions, but rather to focus on "suspicious" transactions – i.e. if the institution has reasonable grounds to suspect that the customer's activities are related to money laundering or terrorist financing. This would increase the quality of the reports while reducing their number, allowing the Financial Intelligence Unit – the Netherlands (FIU-NL) to concentrate on the quality of the transmission to investigative bodies. This would also allow the Netherlands to deviate less from the international practice of primarily reporting suspicious transactions.

Pooling data (provided that privacy and other safeguards are in place) would be helpful in detecting suspicious transactions and improving risk assessments. For example, five Dutch banks are working together under the name "Transaction Monitoring Netherlands" to monitor their transactions for signs of money laundering and terrorist financing. It would be desirable to expand the possibilities for cooperation and data exchange between institutions, in combination with appropriate privacy and other safeguards. Such cooperation would also boost the efficiency of transaction monitoring if institutions were allowed to outsource this work (while retaining responsibility for the work themselves). Section 10 of the *Wwft* currently prohibits this; we would support amending this section of the Act as formulated in the legislative proposal for the action plan to tackle money laundering.

More extensive feedback from FIU-NL to banks would increase their motivation to report unusual transactions while also making the reports more effective. Banks have begun taking their gatekeeper role more seriously, as evidenced by the rising number of reports of unusual transactions to FIU-NL, for example. To improve the effectiveness of their analyses, banks would benefit from feedback from FIU-NL on the agency's grounds for designating transactions as suspicious. This would allow banks to take a more targeted approach when searching for transactions that may be related to money laundering or the terrorist financing, which would in turn boost effectiveness throughout the chain. Feedback loops further down the chain can also serve to increase effectiveness.

Introduction

Everyone in Dutch society should have confidence in the financial sector's fight against financial crime – in particular money laundering and terrorist financing – while also being assured that the services they expect from financial institutions will not be jeopardised. There is great societal urgency to actively prevent and combat financial crime. Indeed, money laundering undermines public confidence in the financial sector. Criminal and terrorist organisations and individuals use laundered money for their own benefit and to finance additional activities. Ultimately, law-abiding citizens pay the price. They are confronted not only with higher taxes, but also with a society that is less safe and in which the rule of law is undermined.

As the supervisory authority, De Nederlandsche Bank (DNB) ensures that institutions have the necessary procedures and measures in place to prevent and combat financial crime. In this way we help create a clean and ethical financial sector. The need for these efforts remains undiminished. Both society and lawmakers call for a firm and effective approach to combating financial crime. We have therefore designated this topic as one of our top three supervisory priorities.

This report focuses in particular on the supervision of banks, which play a pivotal role in the financial system. Enforcement actions and remediation processes have increased banks' efforts to prevent money laundering and terrorist financing. They have become stricter at the gate: banks subject their customers to more intensive scrutiny as part of their due diligence processes, thus allowing for better management of risks. However, these activities also have an impact on the services banks provide. We regularly receive signals indicating that it has become difficult for certain entities and consumers to access or retain banking services.

Against this background, DNB has prepared this report in which we examine our supervisory activities and policy on the prevention of financial crime by banks.[1] In addition to desk research, we also conducted interviews with stakeholders. Moreover, we collected additional information by means of a questionnaire answered by the four largest banks in the Netherlands and we reached out to bank customers who had contacted our Information Desk. In order to increase the effectiveness and efficiency of activities to prevent and combat financial crime, it is important to consider how the efforts of the sector can become truly risk-based and how our own risk-based supervisory activities can contribute to this development. We also intend to discuss the findings of this report during round-table meetings with the sector and other stakeholders.

Following an introductory discussion of the topic in Section 1, we successively discuss the role of banks in preventing and combating money laundering and terrorist financing and the potential side effects (Section 2), our supervisory activities (Section 3), the perspective offered by technological developments (Section 4) and the need for intensive cooperation by all parties involved (Section 5).

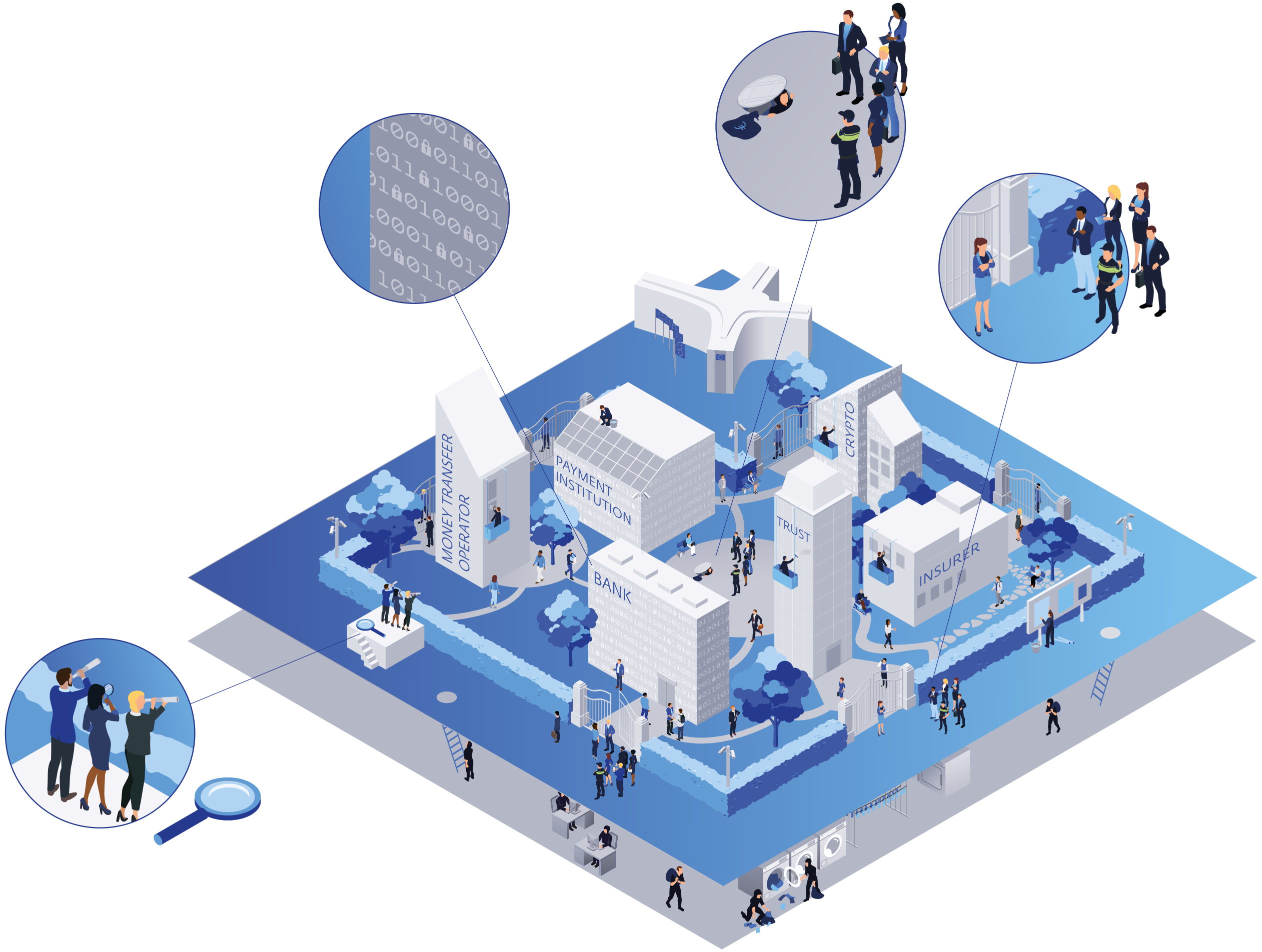
[1] This report focuses on the role of banks in preventing and combating money laundering and terrorist financing. The report does not cover other integrity risks such as compliance with sanctions legislation, neither does it cover the role of non-banking institutions.

1 The scale of money laundering and terrorist financing and the fight against them

1.1 Money laundering and terrorist financing in the Netherlands

Criminal money flows are a problem in society. Criminals launder the proceeds from their illicit activities in order to use the funds in the legal economy. The point of money laundering is to give criminal money a veneer of legality. The subversive influence of organised crime in the Netherlands is a cause for concern, and the underlying financial flows are an important element in this regard. Terrorist financing is a specific form of financial crime that makes use of the financial infrastructure. Terrorist financing is an umbrella term for practices that aim to facilitate all forms of assistance to terrorist activities.

Money laundering is extensive. By its very nature, the exact extent of money laundering and terrorist financing is difficult to assess. Estimates indicate that between two and five percent of global gross domestic product is laundered on an annual basis.[2] As study into the amount of criminal money earned in the Netherlands estimates it at EUR 16 billion annually.[3] According to this study, about half of the money made its way abroad, but an estimated amount of nearly EUR 5 billion of criminal money from abroad also found its way to the Netherlands. The robust digital and physical infrastructure and the quality of the legal and financial services sector in the Netherlands are not only



[2] M. Tiwari, A. Gepp & K. Kumar (2020), A review of money laundering literature: the state of research in key areas, Pacific Accounting Review, Vol. 32 No. 2, p. 271-303.
[3] Bijna €13 mrd wordt er jaarlijks witgewassen in Nederland (fd.nl) (Nearly EUR 13 billion laundered annually in the Netherlands). Based on data from FIU-NL for the period 2009-2014. See also B. Unger et al. (2018), Aard en omvang van criminele bestedingen 2018 (wodc.nl) (Nature and size of criminal expenditure 2018).

beneficial for the regular economy, but are also attractive for those wishing to launder their illicit funds. Publications such as the Panama Papers, the Paradise Papers and FinCEN Files show that money laundering is relatively common in the Netherlands. Less is known about the extent of terrorist financing. The Dutch National Risk Assessment Terrorism Financing 2019 describes 12 criminal convictions for providing financial support to friends or family members who travelled to conflict zones where terrorist activities were taking place. In 2020, FIU-NL registered 4412 suspicious transactions related to terrorism, which is more than 4% of the total number of suspicious transactions.[4]

Preventing and combating money laundering and terrorist financing is of international concern. The recommendations of the Financial Action Task Force (FATF), an influential international organisation of which the Netherlands is a member, provide the basis for the approach to preventing and combating money laundering and terrorist financing. There is also broad cooperation at the European level (see also Section 3). An international approach to financial crime is essential because money also flows between countries, cross-border concealment schemes are being set up and organisations that undertake criminal activities or engage in terrorist financing often operate internationally. International evaluations are carried out on a regular basis to promote the consistency and effectiveness of national policies to combat money laundering and terrorist financing. Three such evaluations took place in the Netherlands in 2021-2022 (see Box 1).

Box 1 International evaluations of Dutch anti-money laundering/anti-terrorist financing policy

The Financial Action Task Force (FATF) carried out an evaluation of Dutch policy to combat money laundering and terrorist financing in 2021-2022 (FATF (2022), The Netherlands - Mutual Evaluation Report. The FATF is the intergovernmental organisation that sets international standards, which are then transposed into national (and European) regulations. In its assessment, the FATF notes that the Netherlands has made significant improvements in its framework, and is in compliance with FATF standards. Strengths include the degree of national cooperation and coordination, both from a policy and operational perspective, and the use of data and intelligence. Points for improvement include tackling the abuse of legal entities and strengthening risk-based supervision.

The Council of Europe, on behalf of the European Commission, is evaluating how EU Member States are implementing the obligations arising from the Fourth Anti-Money Laundering Directive in practice. An anonymised EU-wide report will be published in 2022.

Together with six supervisory authorities from other EU Member States, we underwent an AML/CFT implementation review by the European Banking Authority (EBA) in 2021. The review focused on the effectiveness of the AML/CFT supervision of banks. A summary report (anonymised) on the seven countries concerned will be published in 2022.

We attach great importance to these evaluations. We put a great deal of effort into the preparations, and we will incorporate the recommendations into our supervisory approach.

[4] Annual review FIU-the Netherlands 2020.

Despite the policy framework with global regulatory recommendations, effectively combating financial crime remains a challenge. It is estimated that authorities worldwide seize 0.05% of illegally obtained funds.[5] In the Netherlands, the Public Prosecution Service confiscated EUR 291 million (i.e. 1.8% of the aforementioned EUR 16 billion) in 2021.[6] This suggests that proportionally more money is confiscated in the Netherlands than worldwide. At the same time, 1.8% is still a relatively low figure.

1.2 Preventing and combating financial crime

The Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (*Wwft*) forms the legal basis. In the Netherlands, the European Anti-Money Laundering Directive (AMLD) is implemented in the *Wwft*. The AMLD is a European directive aimed at preventing the misuse of the financial system for money laundering and terrorist financing. The Directive is formulated in accordance with FATF recommendations. The *Wwft* states that institutions must prevent criminals from using their services to introduce illicit funds into the financial system. In brief, the institutions do so by: 1) conducting due diligence on new and existing customers; 2) monitoring transactions; and 3) reporting unusual transactions to FIU-NL. The institutions thus act as “gatekeepers”: they prevent assets with criminal origins from blending into the financial system and they help to detect and stop illicit financial flows that have managed to enter the system.

Customer due diligence procedures establish the identity of (potential) customers, where their money comes from or goes to, and what the money is used for. An institution collects information about its customers to this end. The *Wwft* prescribes the result of customer due diligence, while the institution itself determines how it goes about achieving this result. If the customer due diligence procedure fails to provide sufficient clarity on the customer, its identity and the origin of its funds, or if the estimated risk of criminal origin or criminal use is too high, the institution may not provide services to this customer. Criminals and other wrongdoers are thus turned away at the gates of the financial system.

Transaction monitoring is used to detect and report unusual transactions: those that do not fit into the usual pattern of an account. An institution determines whether a transaction is unusual by means of a list of objective indicators on the one hand. These indicators may vary from one category of institution to another. Often, the indicators are characteristics such as a transaction exceeding a certain threshold. On the other hand, analysts at an institution can judge whether a transaction is unusual based on their expert opinion: the transaction does or does not give reason to suspect that it may be related to money laundering or terrorist financing. This results in so-called “subjective reports”. Institutions subject to the *Wwft* reported 1.2 million unusual transactions to FIU-NL in 2021 (Table 1).[7] Over 50% of the reports came from payment institutions (including money transfer institutions), 25% from crypto service providers and over 20% from banks. The remaining reports came from a diverse range of other gatekeepers, such as foreign exchange service providers, crypto exchanges, accountants, notaries and car dealers.

[5] R. Pol (2020), Anti-money laundering: The world's least effective policy experiment? Together, we can fix it (tandfonline.com), Policy Design and Practice, 3:1, p. 73-94.
[6] Openbaar Ministerie Jaarbericht 2021 (Public Prosecution Service Annual Review 2021), Key figures 2021, table on Confiscation.
[7] 2021 Annual review of FIU-the Netherlands.

Table 1 Number of transactions categorised as unusual and suspicious

	2017	2018	2019	2020	2021
Unusual transactions	361.015	394.743	541.236	722.239	1.230.411
of which reported by:					
banks	22.789	67.524	147.952	245.143	262.991
payment service providers	309.619	291.589	350.775	422.878	638.218
crypto service providers				7.309	301.928
other	28.607	35.630	42.509	54.218	27.274
reported on the basis of:					
subjective indicators	68%	69%	59%	57%	45%
objective indicators	32%	31%	41%	43%	55%
Suspicious transactions	40.546	57.950	39.544	103.947	96.676
of which reported by:					
banks	4.163	15.437	12.919	40.382	47.325
payment service providers	33.533	39.239	21.996	56.866	38.513
crypto service providers				3	5.860
other	2.850	3.274	4.629	6.699	4.978

Source: FIU-NL Annual Reviews 2019, 2020, 2021. Not included: "legal indicator objective 02" (the list of risk countries designated by the European Commission).

Significant improvements have been made in recent years in combating money laundering and terrorist financing. The Netherlands Court of Audit has concluded that clear progress has been made in this area.[8] This is reflected, for example, in the increased level of activity throughout the chain. In 2021, institutions reported three and a half times as many unusual transactions as in 2017; the number of transactions identified by FIU-NL as suspicious increased by 138% in the same period. There has also been a significant increase in the number of money laundering offences handled by the Public Prosecution Service (up 155% between 2017 and 2021[9]) and the number of convictions in court (from approx. 600 convictions in 2016 to approx. 1100 convictions in 2020[10]).

Increased efforts by banks have resulted in a significant increase in the number of reports they submit. Banks have significantly increased their capacity in this area in recent years. Partly because of this, banks reported 1054% more unusual transactions to FIU-NL in 2021 than in 2017. The number of transactions originating from banks that FIU-NL designated as suspicious also increased by 1036% during this period.

[8] Netherlands Court of Audit (2022), Combating money laundering part 3: state of affairs 2021.
[9] Openbaar Ministerie Jaarbericht 2021 (Public Prosecution Service Annual Review 2021), Key figures 2021, table Inflow of criminal cases.
[10] Netherlands Court of Audit (2022), Figure 5.

In addition, gaining access to the banking sector has become more difficult. Access to the banking infrastructure has become much stricter. Banks have tightened their policies on customer acceptance and terminating customer relationships. This is also reflected in the increase in the number of complaints and court cases challenging banks' decisions. We surveyed a number of banks for this report in order to gain more insight into these stricter policies (see Section 2). Through this fact-finding exercise, we hope to contribute to a debate on preventing and combating money laundering and terrorist financing that is based more on objective facts and less on subjective anecdotes.

The academic literature reveals cautiously positive effects of anti-money laundering policies. For example, research in the Netherlands shows that the 2015 introduction of the Fourth Anti-Money Laundering Directive (AMLD4) made things more difficult for money laundering networks.[11] The scholarly consensus is that the Directive has made it harder for criminals to launder money, meaning that they must now search for new methods, alliances and structures to achieve their goals. Research also shows that the AMLD4 has had a positive effect on the market valuation of European banks.[12] The application of anti-money laundering regulations has also been shown to have a positive effect on the development of the financial sector.[13] Moreover, a study conducted in nearly 100 countries shows that anti-money laundering regulations have a verifiably downward effect on how much money is laundered.[14]

We supervise compliance with the Wwft by financial institutions such as banks, insurers, trust offices, crypto service providers and payment institutions. The other *Wwft* supervisors are: the Dutch Authority for the Financial Markets (AFM), the Financial Supervision Office (BFT), the *Wwft* Supervision Office (BT*Wwft*), the Netherlands Gaming Authority (Ksa) and the deans of the Netherlands Bar (NOvA). Together, these supervisory authorities form the administrative law chain in the fight against financial crime. Relevant authorities in the criminal law chain are also involved: FIU-NL, the Fiscal Intelligence and Investigation Service (FIOD), the police and the Public Prosecution Service (OM). FIU-NL analyses the reports it receives from the gatekeepers. Of the 1.2 million reported unusual transactions in 2021, almost 97,000 were classified as "suspicious". FIU-NL classifies transactions as suspicious on the basis of its own investigations and as a result of hits with the police, the Public Prosecution Service and the Central Fine Collection Agency (CJIB). These suspicious transactions are passed on to investigative bodies such as the FIOD and the police, who investigate whether criminal acts may have been committed. The Public Prosecution Service decides whether or not to prosecute. The participants in the administrative law chain and the criminal law chain are collectively known as the chain partners. They strive for an integrated approach to detecting and fighting financial crime (Figure 1).

[11] P. Gerbrands, B. Unger. M. Getzner & J. Ferwerda (2022), The effect of anti-money laundering policies: an empirical network analysis (springeropen.com), EPJ Data Science, 11:15.
[12] A. Premti, M. Jafarinejad, & H. Balani (2021), The impact of the Fourth Anti-Money Laundering Directive on the valuation of EU banks | Elsevier Enhanced Reader, Research in International Business and Finance, 57.
[13] I. Ofouda, J. Abor, J & E. Agbloyor (2020), Anti-money laundering regulations and financial sector development, International Journal of Finance & Economics.
[14] A. Chong & F. Lopez-De Silanes (2015), Money Laundering and Its Regulation, Economics & Politics, Vol. 27 Issue 1.

Non-compliance with the *Wwft* can have consequences under both administrative and criminal law. The supervisory authority can intervene under administrative law, primarily to compel the institution to engage in remedial activities to restore compliance with the *Wwft*. To this end, the supervisory authority also has formal (legal) instruments at its disposal, such as instructions or orders subject to penalty. Pursuant to one of the latest amendments to the *Wwft*, the supervisory authority is required to disclose any formal measures it imposes. This also applies to fines, which are moreover punitive in nature. Non-compliance with *Wwft* provisions can also qualify as an economic offence, which means that, in the event of a fine, a choice must be made between proceedings under criminal or administrative law. The choice of criminal or administrative law may depend on the gravity of the economic offence. Criminal law is more expedient in cases of intent or gross negligence. The Public Prosecution Service has primacy in this regard.

Cooperation between chain partners is essential for preventing and combating money laundering and terrorist financing. The Financial Expertise Centre (FEC) is one of the oldest partnerships for combating financial crime. The chain partners mentioned above all work together in the FEC, which facilitates information exchange, knowledge transfer and joint projects. The public partners have been cooperating in the FEC for some time already, and a number of large financial institutions have joined them in recent years. One example is the Serious Crime Task Force, in which the police, the Public Prosecution Service, FIU-NL and the FIOD work together with a number of large banks to tackle subversive crime.

1.3 A risk-based approach

A risk-based approach is at the heart of the international and national frameworks for preventing and combating money laundering and terrorist financing. Based on a risk analysis, countries should adopt a risk-based approach that ensures that measures to prevent money laundering and terrorist financing are proportionate to the risks identified.[15] Where higher risks are identified, countries should address them in the regulatory framework with correspondingly strict measures. Where risks are lower, simpler measures will suffice. This risk-based approach also serves as the basis for European (AMLD) and Dutch (*Wwft*) regulations.[16] For example, the *Wwft* stipulates that, on the basis of a basic examination (see also Section 2), an institution must verifiably adjust its customer due diligence to the risk sensitivity for money laundering or terrorist financing for each type of customer, business relationship, product or transaction. Supervisory authorities must also carry out their duties in a risk-based manner (see also Section 3).

[15] See, for example, the FATF recommendations and the EBA guidelines.
[16] See, for example, the explanatory memorandum to the amendment of the *Wwft* Parliamentary Papers II 2018/2019, 2019 35245, no. 3 (in Dutch).

A risk-based approach is also common among supervisory authorities in a broader sense. The core idea is that the greatest supervisory emphasis is on the highest risks, and that supervision becomes more effective if the supervisory authority's resources are focused on precisely these high risks. Supervisory expert Malcolm Sparrow describes this as follows: "Pick important problems, fix them, and then tell everyone".[17] This ensures greater societal impact and more effective use of the supervisory authority's limited capacity. Or, as the Scientific Council on Government Policy states: *"The idea behind risk-based supervision is that the supervisor no longer checks all supervised organisations, but only looks at a selection of them on the basis of risk analysis and risk profiles. Supervision becomes more intense as the risks increase."*[18]

The risk-based approach broadly consists of three steps:

- *Identifying risks*: in this phase, the supervisory authority looks at potential risks to public objectives that arise from its (legal) mandate.
- *Classifying risks*: once risks have been identified, they must be classified in order to determine which risks the supervisory authority will prioritise. Often, this involves looking at both the impact the risk can have (how much damage can be done to public objectives?), and the likelihood of the risk occurring (is it a "black swan" risk, or is it almost certain to happen?).
- *Mitigating risks:* once the risks have been prioritised, the supervisory authority will look at which instruments to use to compel the institution concerned to manage these risks. This sometimes means that informal interventions are considered first before "heavier" enforcement measures are applied. However, there may also be a reason to immediately implement a heavier measure.

We endorse this risk-based approach and we base our activities on it when supervising compliance with the Financial Supervision Act (*Wet op het financieel toezicht – Wft*) and the *Wwft* (see also Section 3).

[17] M. Sparrow (2000), The Regulatory Craft: controlling risks, solving problems and managing compliance. Brookings Institution.
[18] WRR (2013),Toezien op publieke belangen. Naar een verruimd perspectief op rijkstoezicht (Supervising the public interest. To a broader perspective on national supervision).

2 The role of banks as gatekeepers

Banks are important gatekeepers because they provide access to essential financial services and are at the heart of the financial transaction system. Banks are involved to a greater or lesser extent in almost every financial transaction. The measures that banks take to counter misuse of banking services can therefore make a significant contribution to preventing and combating money laundering and terrorist financing. This means they have a great responsibility. As banks fulfil their gatekeeper role, law-abiding citizens and bona fide companies are also affected by the measures they take. The aim is to compromise service to these citizens and businesses as little as possible.

Banks and customers provided information to us to help us prepare this analysis. We conducted a survey among the four largest banks in order to gain insight into the way they fulfil their gatekeeper role, the associated costs and the consequences for customers.[19] We also held discussions with these banks and some other stakeholders. The remainder of this section draws mainly on the results of this survey. In addition, we used information from bank customers who contacted our information desk about anti-money laundering and anti-terrorism measures in the first half of 2022. We asked these customers by telephone for further information about their experiences.

2.1 Efforts by banks to combat money laundering and terrorist financing

In recent years, we have found that part of the banking sector has failed to comply sufficiently with the *Wwft*. As a result, we have repeatedly had to take enforcement action, and some banks have also faced criminal prosecution proceedings, resulting in significant penalties. Remediation processes are in place at 28 banks - including the larger ones - to address the shortcomings in their customer due diligence procedures and in their procedures for monitoring and reporting transactions.[20]

Banks have now significantly increased their efforts and investments in this area. According to the results of the above-mentioned survey, the costs associated with combating money laundering and terrorist financing accounted for 8% of the total administrative costs of the four largest banks in 2021. This amounted to more than EUR 1.1 billion, a quarter of which was attributable to remedial processes. The vast majority of the costs are wage costs for the more than 10,000 FTEs dedicated to the prevention of money laundering and terrorist financing.[21]

The increased efforts are also reflected in the number of reports of unusual transactions. Whereas banks reported almost 23,000 unusual transactions to FIU-NL in 2017, by 2021 this figure had risen to almost 263,000 (see Table 1 in Section 1). Banks find, however, that FIU-NL is slow to follow up on these reports and that the reports do not, or hardly ever, result in actual criminal proceedings. The banks also indicated that the feedback from FIU-NL does not provide them with sufficient guidance to revise their policies, procedures and measures. To improve the effectiveness of their analyses, banks would benefit from feedback from FIU-NL that specifically indicates why transactions are designated as suspicious and, where possible, what results were achieved by investigating the reported transactions.

[19] These are the four largest banks measured by the number of customers. A survey on the same topic was conducted in 2016. The results are comparable to only a limited extent, and only a few points are compared here.
[20] DNB letter to the Minister of Finance on the case of ABN Amro Bank NV.
[21] For the banking sector as a whole, the costs in 2021 amounted to nearly EUR 1.4 billion, and the number of FTEs was nearly 13,000.

Bank customers also notice that banks have tightened their policies. For example, banks now request more information from their customers and they are more likely to terminate relationships with customers who do not provide the requested information or who fall outside the bank's risk appetite. Consequently, the number of potential customers who are not accepted and the number of customers whose banking relationship is terminated by the bank has been on the rise since 2016. We discuss these consequences below.

2.2 Consequences of banks' tighter policies

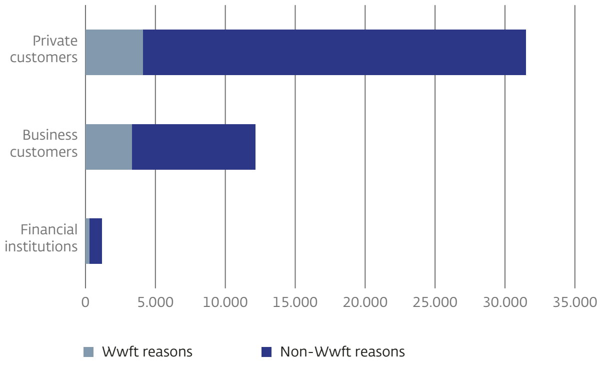
2.2.1 Consequences for customer acceptance

As part of their role as gatekeepers, banks prevent criminal money flows from entering financial system. Banks may decide not to accept potential customers or to stop providing certain services to customers whose risk of involvement in such money flows is too high. This is in keeping with their responsibility as gatekeepers of the financial system. In accordance with the spirit of the *Wwft*, such decisions must be based on a risk assessment. Indeed, a bank cannot determine with full certainty whether a customer's transactions involve criminal flows of money. The bank must conduct a risk assessment and act accordingly. Underestimating the risks may inadvertently facilitate money laundering or terrorist financing. At the same time, customers may also be turned away unnecessarily. This unnecessary "de-risking" is undesirable because it deprives bona fide customers of access to essential financial services.

Banks often terminate customer relationships for reasons other than money laundering or terrorist financing risks. In 2021, the four banks surveyed terminated relationships with nearly 45,000 customers. (Figure 1) In 17% of cases (7,700 customers), this was because of the risk of money laundering or terrorist financing. This number is roughly twice as high as in 2016, and most of these customers fell in the business segment. Examples of such "*Wwft* reasons" are that a customer falls outside a bank's risk appetite or refuses to cooperate with the customer due diligence procedure. The banks terminated relationships with more than 4,100 private individuals in 2021, which is 0.02% of the total number of private customers at the end of 2020.[22] The banks terminated relationships with 3,600 business customers (including financial institutions) for "*Wwft* reasons" in 2021, which is 0.17% of the total number of business customers. Besides the "*Wwft* reasons", banks may have other reasons to end customer relationships such as involvement in fraud and, in the case of business customers, not fitting in (or no longer fitting in) the bank's commercial policy or because of environment-related or societal factors. The latter includes risks of serious environmental damage or human rights violations.

Figure 1 Number of customer relationships terminated in 2021

Broken down by underlying reasons



Note: based on data from the four largest banks. *Wwft* reasons: customer does not fit within integrity risk appetite with regard to *Wwft* compliance, customer non-cooperative, bank could not meet legal requirements with regard to customer due diligence, other *Wwft* reason Non-*Wwft* reasons, including fraud, reputation risk to the bank, commercial reasons and environmental or societal factors.

When customer relationships are terminated, there appears to be little connection to the risk category in which an individual customer was classified, which may be indicative of a flawed risk classification. Banks conduct customer due diligence to assess the risk of a customer being involved in money laundering or terrorist financing. This is the basis on which they are assigned to a risk category: low or reduced, moderate or normal, and high or increased. In addition, there is the "unacceptable" category; the relationship with customers in this category will be

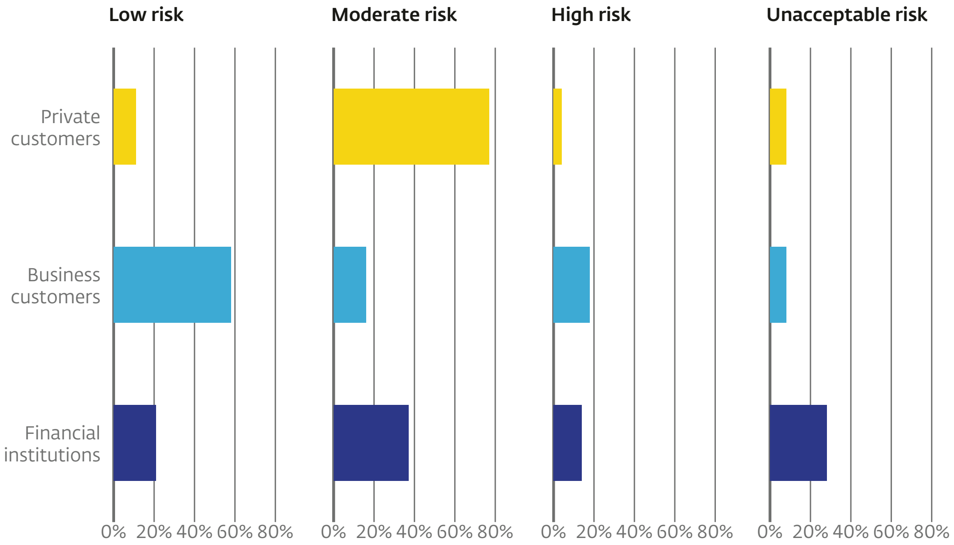
[22] An individual or a company may be a customer at several banks. This customer will therefore appear at several banks as an existing customer or as a customer with whom the relationship has been terminated.

terminated as soon as possible. The distribution by risk category of bank customers whose relationships were terminated in 2021 for *Wwft* reasons reveals that many of these customers were not assessed as high risk, but as low or moderate risk (Figure 2). Money laundering and terrorist financing risks were thus also identified among customers initially classified as low or normal risk.

Customer relationships with financial holding companies, construction companies, transport companies and wholesalers were terminated relatively often due to risks of money laundering and terrorist financing (Figure 3). Relative to the total number of bank customers in these sectors, this occurred in fewer than 0.5% of cases. Although the number of terminations is limited compared to the total customer base, the number of terminations varies between sectors. Customer relationships with financial holding companies were terminated most frequently (374 cases), followed by the construction sector (231 cases), the transport sector (153 cases) and wholesalers (151 cases). In relation to the total number of customer relationships in the relevant sector, this is 0.13% for the construction industry and 0.42% for the transport sector.

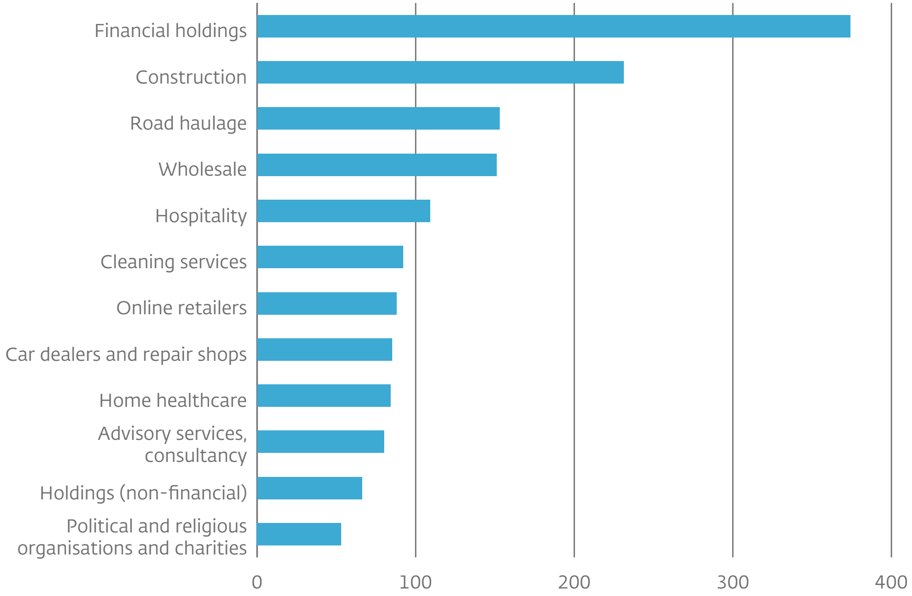
Figure 2 Distribution by risk category of bank customers whose relationships were terminated in 2021 for *Wwft* reasons

As a percentage of customer groups



Note: based on data from the four largest banks.
The totals add up to 100% for each customer group.

Figure 3 Number of business customers whose bank relationships were terminated in 2021 for *Wwft* reasons by sector



Note: based on data from the four largest banks. Refers to the 12 largest sectors in terms of the number of customer relationships terminated. In some cases, smaller sectors are clustered.

The reason for terminating services varies from case to case. Customer characteristics that frequently arise as potential reasons for terminating a relationship include negative reports about the customer in the media or other sources, or increased risks due to complex, unusual or unexpectedly large transactions. Another frequently mentioned customer characteristic applies to those who operate in sectors with an increased risk of money laundering or terrorist financing, or those with ties to jurisdictions that have an increased risk of money laundering and/or terrorist financing. Finally, in a number of cases customers refuse to provide the requested information or documentation or they do not have sufficiently clear ties to the Netherlands.

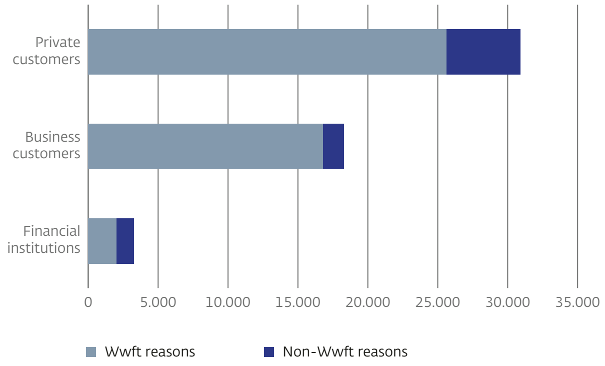
Although the *Wwft* requires that the bank *must* terminate the relationship in certain cases, this is not always feasible in practice. Case law in this area is developing, but banks see that customers who challenge the termination of their banking relationship in court are successful relatively often: the fact that banks have a utility function and that customers are likely to encounter difficulty opening an account elsewhere means that the courts regularly (but certainly not always) prohibit banks from terminating customer relationships. The bar for terminating the relationship is set high, which means banks must take their gatekeeper role all the more seriously. Banks do not have a clear picture of where customers go when relationships are terminated; some customers hold accounts elsewhere and may continue their relationships with those banks.

Terminating a customer relationship is a relatively heavy means to deal with *Wwft*-related risks, which is why banks sometimes choose to limit their services instead. Around 52,000 customers fall into this category. The reason for limiting services is *Wwft*-related in the majority of cases (83% private individuals, 92% business customers and 62% financial enterprises; Figure 4). This group comprises nearly 26,000 private and nearly 19,000 business customers (including financial enterprises). This contrasts with the previously cited reasons for terminating customer relationships, the majority of which are *non-Wwft*-related (Figure 1). The risks of money laundering and terrorist financing in particular can often be reduced by limiting services, for example with regard to the use of cash. Limiting service is less appropriate in cases where customers are involved in fraud or work in a sector in which a bank wishes to cease activities for ethical reasons.

There is significant overlap between sectors where services were limited and sectors where services were terminated for *Wwft* reasons. The seven sectors with the most service limitations are also the sectors in which customer relationships were most often terminated. After financial holding companies, enterprises in the hospitality sector were most likely to see services limited (Figure 5). The creation of a "basic bank account" for small business customers may be another avenue for providing services, subject to restrictions, to customers with a high risk profile. Individuals already have the right to a basic bank account, and persons to whom this legal right does not apply (e.g. due to conviction for a financial crime) may still open an account under the Basic Bank Account Covenant.

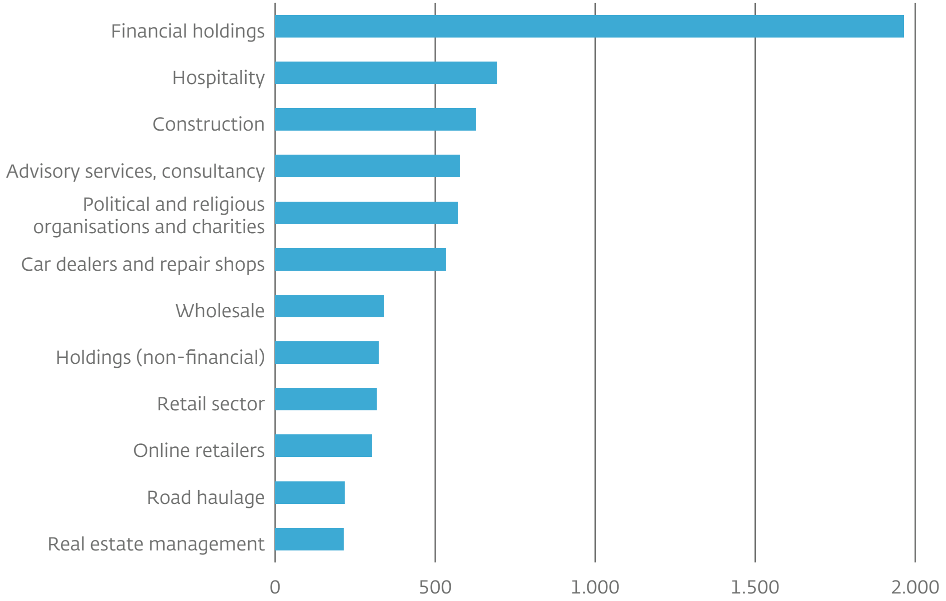
Figure 4 Number of customers whose services were limited in 2021

Broken down by underlying reasons



Note: based on data from the four largest banks. *Wwft* reasons: customer does not fit within integrity risk appetite with regard to *Wwft* compliance, customer non-cooperative, bank could not meet legal requirements with regard to customer due diligence, other *Wwft* reason Non-*Wwft* reasons, including fraud, reputation risk to the bank, commercial reasons and environmental or societal factors.

Figure 5 Number of customers whose services were limited in 2021 for Wwft reasons by sector

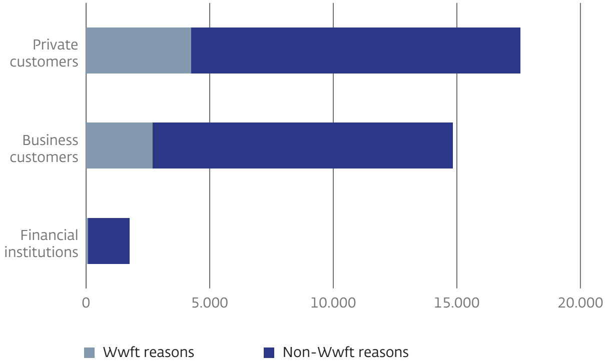


Note: based on data from the four largest banks. These are the 12 largest sectors in terms of the number of customers. In some cases, smaller sectors are clustered.

Banks did not accept approximately 34,000 potential customers in 2021. Alongside customers whose banking relationship was terminated, there is another group who were not accepted at all. This group is estimated to comprise about 18,000 individuals, 15,000 business customers and 1,750 financial institutions (Figure 6). As in the case of termination of existing customer relationships, potential customers are rejected less often for *Wwft* reasons: an estimated 25% private individuals, 18% business customers and 4% financial enterprises. Common characteristics of potential customers that were rejected for *Wwft* reasons include incomplete or incorrect documentation, unwillingness to cooperate with information requests, not fitting in with the bank's risk appetite or insufficient ties to the Netherlands. Here, too, the number of rejections increased compared to 2016. A breakdown by sector is not possible based on the available data. It is largely unknown whether these rejected customers were accepted at another bank. However, anecdotal evidence suggests that customers rejected by one bank try their luck at other banks (the "waterbed effect"). No data is available on numbers of customers who were not rejected outright yet who were deterred by the administrative burden of the due diligence procedure.

Figure 6 Number of potential customers rejected in 2021

Broken down by underlying reasons



Note: based on data from the four largest banks. The data is incomplete and partly estimated. *Wwft* reasons: client does not fit within integrity risk appetite with regard to *Wwft* compliance, client non-cooperative, bank could not meet legal requirements with regard to client screening, other *Wwft* reason Non-*Wwft* reasons, including fraud, reputation risk to the bank, commercial reasons and environmental or societal factors

2.2.2 Burden on customers

Although bank customers consider it important to combat money laundering and terrorist financing, they are at the same time dissatisfied with requests for information they receive from their banks. This is revealed by reports submitted to our Information Desk and through other channels. Banks need information to get to know their customers and thus determine the extent of the risk of money laundering or terrorist financing. However, some customers experience these information requests as an unwanted burden, they find the questions to be too intrusive and in some cases they feel they are being asked to prove their innocence. They also find it annoying when they are required to submit the same information more than once.
They would prefer it if institutions could simply rely on each other's assessments, or if they could give permission for institutions to share data.

Banks say that they need the requested information in order to comply with the *Wwft*. They also say that their requests for information are in line with the risk-based approach of the *Wwft*. This is reflected, among other things, in the fact that the burden on private customers is generally less than on business customers. This applies in particular to private individuals with a low risk profile; banks will generally have no reason to request additional information from these types of customers. As soon as a customer's risk profile changes, the requests for information become more frequent and the level of detail of the information requested increases. In exceptional cases, the number of documents requested can grow substantially.
Banks would like to make more use of public registers (municipal personal records database, UBO register) in order to reduce the need to ask customers themselves. Both customers and institutions would benefit if information could be reused more easily by multiple institutions.

The burden on the customer differs per bank, especially for business customers. Some banks initially request a limited set of documents, while others ask for more extensive information straight away. Additional information may be requested depending on various factors, including customer characteristics and the availability of documents from public sources. As with private customers, the riskier a potential customer is, the greater the information burden will be. Small business customers in particular experience this as a high burden.

Banks are also struggling with the risk-based approach. In some situations, banks have difficulty explaining exactly why they request certain information, while at the same time they feel that the *Wwft* compels them to request further information from the customer, some of which can be quite invasive. Banks thus take a rule-based approach to satisfying the open standard for fear of not complying with the law and being called to account by the supervisory authority. An example of this is requests for information from politicians (and even their children) or other persons in authority[23], while the risk profiles of these individuals in many cases do not warrant the collection of additional information. Another example

[23] Politically Exposed Persons (PEPs).

is when a bank, when accepting a new customer, must draw up an expected transaction profile based on information provided by the customer. A bank would generally prefer to identify any unusual transaction patterns by other means, such as by classifying the customer in a peer group with an associated standard profile.

Banks request less information when reviewing current customers than when performing due diligence on new customers. In principle, banks conduct both periodic reviews and reviews based on signals. The higher the customer's risk profile, the more information banks request during periodic reviews. Banks often only review customers with the lowest risk profile if they have received a concrete signal to do so. Examples of signals that may trigger a review are deviations from the expected transaction pattern, increased or high cash payments or deposits or activities that deviate from expected activities within a certain sector.

The review process is relatively burdensome for some sectors. This pertains in particular to sectors that banks generally consider to be high risk such as commercial real estate, scrap dealers, trust companies and foundations. The high risk rating means that they are subject to much more frequent periodic reviews and the associated information requests are more penetrating. The latter aspect also applies to the acceptance phase.

Information from notifications submitted to us reveals that multiple customers feel that banks request unnecessary information or information that they feel uncomfortable sharing.[24] In various notifications, customers state that it was unclear why banks requested certain information, both during initial due diligence and during later reviews. The banks wished to see tax returns, balances with other banks and information from the distant past, for example. Customers are surprised by requests for information, especially when they have been customers for a long time and they expect the bank to have the information already available or to be able to obtain it from another source. Almost all customers who spoke with us endorse the importance of preventing money laundering and terrorist financing and are also prepared to do what is expected of them. Nevertheless, they experience the approach as rigid and coercive. Finally, they are concerned about privacy and fearful that sensitive information might end up in the wrong hands.

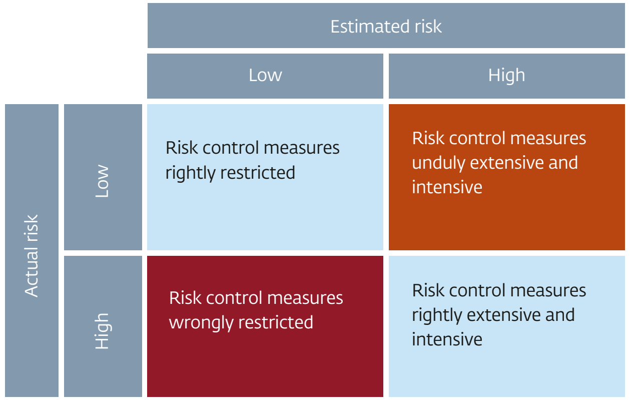
2.3 Strengthening the risk-based approach

The *Wwft* is risk-based legislation: the intensity of measures to prevent money laundering and terrorist financing should be tailored to the concrete risks posed by a customer. The higher the risk posed by the customer, the more scrutiny is called for; if the risk is lower, less intensive monitoring will be sufficient.

The risk analysis is and will remain the premise for managing risk. If a bank has a good understanding of the integrity risks it runs, both within its own organisation and among its customers, it can base its approach on these insights. An inadequate risk analysis can have various consequences, which are summarised in Figure 7. A bank can make two types of misjudgements in this process. On the one hand, underestimating the risks can cause a bank to take too few risk control measures (the red area). On the other hand, overestimating the risks can lead to banks taking too many measures that are also too intensive (the orange area).

[24] Based on a telephone survey of 31 people who contacted our Information Desk in the first half of 2022.

Figure 7 Actual risk and estimated risk



		Estimated risk	
		Low	High
Actual risk	Low	Risk control measures rightly restricted	Risk control measures unduly extensive and intensive
	High	Risk control measures wrongly restricted	Risk control measures rightly extensive and intensive

If too many customers are wrongly classified as “low” or “high” risk, then this indicates shortcomings in the bank’s rating system. Supervisory authorities closely examine the red area in view of the banks’ gatekeeper role. Such emphasis remains necessary because high-risk customers are the greatest source of potential abuse of the financial system. In addition, a risk-based approach also calls for scrutiny of the orange area. Supervisory authorities also have a role to play in countering “over-compliance”.

Banks do not feel that they have the scope to limit control measures, even if their application is not proportionate in a given case. This is particularly true if a high-risk factor is present (e.g. a PEP or a foundation), but the likelihood of the risk actually materialising is negligible. This is a potential cause of unnecessary de-risking and a disproportionate burden on the customer. Interpreting the *Wwft* too strictly can cause banks to take disproportionate measures, burdening their customers unnecessarily even in the case of low risks. This can potentially undermine the effectiveness of the *Wwft* while also eroding support for compliance with the legislation. Supervision may be similarly affected. More limited measures in the case of low risks creates scope to focus resources on higher risks. Adopting a more risk-based approach such as this can contribute to the effectiveness of efforts to control the risks of financial crime.

The use of cash gives rise to a dilemma. Cash is legal tender, the legitimate use of which should not be hampered. Under certain circumstances, however, the use of cash can be a strong indicator of money laundering or of terrorist financing. At our initiative, organisations closely involved in the Dutch payment system concluded a new Cash Covenant in April 2022.[25] In the context of this Covenant, we formulated a number of considerations to be kept in mind when taking measures against money laundering and terrorist financing. Indicators for additional scrutiny include transactions involving unusually large sums, remarkable patterns in payment behaviour, the use of large denominations, frequent transactions that may indicate “smurfing” (covering up large transactions by splitting them into multiple smaller transactions) and transactions that do not fit the customer’s profile. Banks will base any measures they deem necessary to prevent money laundering or terrorist financing on a substantiated, customer-specific or customer-group-specific risk assessment. Banks will inform us in good time of their risk assessments and intended measures so that we have the opportunity to discuss this with them.

As we continue to move forward with the risk-based approach and our emphasis on high risks, we also intend to take a closer look at low risks. To this end, we could potentially work together with the sector to arrive at practical guidance based on specific input. The assumption is that, by pursuing a more effective approach, banks will take more measures where needed and fewer where possible. For example, banks might not need to request certain information during a review if the customer’s transaction behaviour does not reveal any increased risk. Banks could also refrain from requesting additional information during the customer acceptance process if, despite the presence

[25] New covenant lays down agreements on proper functioning of cash (dnb.nl).

of a high-risk factor, the actual situation is clearly low-risk in nature. A truly risk-based approach also helps to avoid unnecessary de-risking.

Providing the customer with a full explanation of why the bank requests information and how the bank deals with that information can help the customer understand the need for these measures. Indeed, the enhanced risk-based approach still implies that, for higher risks, banks need to request more information from customers in order to estimate the risk more accurately and to take the most appropriate control measures. Customers may perceive these requests to be annoying and disproportionate. Customers tend to be willing to make an effort to combat money laundering and terrorist financing, which is why it is important that banks clearly explain why they request certain information. It is insufficient to explain that the request stems from a legal obligation under the *Wwft* or that it has been imposed by the supervisory authority; customers need a more substantiated and satisfactory explanation. In this respect, sector organisations and banks could certainly work more closely together on sharper and more specific risk analyses aimed at more targeted risk mitigation. Consultations under the aegis of the National Forum on the Payment System (NFPS) provide a framework to this end. It is also advisable to take concerns regarding the sharing of sensitive data seriously. For example, it is important to use secure channels for collecting information, and customers must be assured that bona fide requests for information are not attempts at phishing. Moreover, customers prefer to be aware of what happens to their data. Clear policies and explanations, in which the bank also provides assurances that information will not be used for other purposes, can help allay concerns.[26]

[26] The GDPR also requires transparency in relation to the processing of personal data.

3 Our supervision of banks’ gatekeeper role

3.1 Supervision focuses on concrete risks

We are committed to risk-based supervision. This requires a proportionate use of supervisory capacity: more intensive supervision of institutions facing high risks due to their size, impact and complexity, and less intensive supervision when the risks are lower. Risk analysis is thus not only essential for institutions, but also for us as a basis for executing our supervisory tasks. This approach also serves as the foundation for our supervisory methodology.[27]

Risk-based supervision is multi-dimensional. First of all, the risks, and therefore the risk profiles, differ from sector to sector. Next, the risk profiles of supervised institutions differ. One bank’s risk profile differs from another bank’s, for example because of the products it offers, the market segments it serves and the jurisdictions in which it operates. Moreover, some customers of an institution may be riskier than others. We take these differences into account when deploying our intrinsically restricted supervisory capacity. We therefore assess the control measures applied by an institution in a given case relative to the specific risk.

To help institutions understand risks and implement their obligations, we regularly issue guidance documents, which are evaluated and revised as necessary. The *Wwft* has a large number of open standards, which can sometimes be challenging for institutions to comply with. We provide guidance on how to comply with these standards. This information function is a key element of our supervisory activities. Alongside clarifying documents from international organisations such as the FATF and EBA, we provide explanation and clarification in guidance documents, good practices, Q&As and news releases. Our “Guidance on the *Wwft* and the Sanctions Act” explains the risk-based approach, customer due diligence, transaction monitoring and reporting of unusual transactions, among other topics. In addition to this general explanatory documentation, there are a number of specific policy documents such as on customer due diligence for foundations, post-event transaction monitoring, the systematic integrity risk analysis (SIRA) and commercial real estate activities.

3.2 Prevention of financial crime as a priority of supervision

Ensuring that institutions prevent and combat financial crime is a priority in our supervisory activities. We re-emphasise this in our “Supervisory Strategy 2021-2024” and in earlier documents on our supervisory strategy.[28]

[27] DNB, Our redesigned supervisory approach.
[28] DNB, Supervisory Strategy 2021-2024 and Supervisory Strategy 2018-2022.

Our mandate under administrative law is evolving. The range of tools available under administrative law has been expanded through the years, including much higher maximum fines for violations of the *Wwft* and the requirement to disclose formal enforcement and punitive measures. These developments buttress our efforts to strengthen the foundation for preventing and combating financial crime and the remediation of shortcomings when they are detected. We will continue to use all means at our disposal to achieve *Wwft* compliance throughout the sector. In addition, the Public Prosecution Service's targeted approach has also had an impact: settlements following criminal proceedings with a number of major banks have sent a clear signal that banks need to get their act together. As the fight against financial crime goes forward, it is essential to consider when to apply criminal law or administrative law; the Public Prosecution Service has primacy in this matter. Against this background, our mandate under administrative law, and by extension our powers and supervisory tools, continue to evolve. We will continue to deploy the full range of tools to ensure that institutions fulfil their gatekeeper role effectively.

Enforcing the *Wwft* standards is a core task of supervision. Enforcement activities are aimed at the core purpose of the *Wwft*: preventing banks and other institutions from becoming involved in money laundering and terrorist financing. The severity of our enforcement measures depends on various factors, including the seriousness and duration of the offence, the degree of culpability and the institution's level of commitment to restoring and maintaining compliance.[29] We decide whether or not to use a formal measure based on these factors. Since 2018, we have been able to impose higher fines for violations of the *Wwft*, which in certain cases can amount to 20% of net turnover. We also disclose administrative sanctions such as orders subject to penalty or administrative fines. We feel that disclosure is important as it increases the effectiveness of these tools by imbuing them with a more pronounced preventive effect.

3.3 Priorities for our supervision in the years ahead

We intend to take the risk-based approach to the next level, both in our supervision and in the risk-based application of the *Wwft* by banks and other institutions. In recent years, our integrity supervision has focused mainly on the preconditions for managing the risks of financial crime. In short, the basis for preventing involvement in money laundering and terrorist financing had to be put in order first. This resulted in various remediation programmes, some of which were extensive.

In the coming years, we will continue to monitor the implementation of arrangements made with banks to remedy shortcomings. In doing so, we will take a risk-based approach to the intensity of our supervision, the assessment of individual situations and enforcement measures. Not every instance of non-compliance will automatically result in a fine, but shortcomings must always be resolved. This will lay the foundation for the further fulfilment of the gatekeeper function.

We see a more robust application of the risk-based approach by banks as the next important priority in supervision. In this context, it is not only important for banks to take more measures in the case of higher risks, but it is also appropriate for institutions to use the scope available for more limited measures in the case of low risks. This means that banks will have to evolve in the application of the risk-based approach and we will face a similar evolution in our supervisory practice. It also means facing up to the fact that a risk assessment, however judicious, may nevertheless potentially result in a decision that, in hindsight, was poor. This does not necessarily indicate a management failure.

[29] See for more detail: AFM and DNB, Handhavingsbeleid van de Autoriteit Financiële Markten en De Nederlandsche Bank (Enforcement policy of the Authority for the Financial Markets and of De Nederlandsche Bank).

Institutions must adopt a holistic view for the risk assessment of the individual customer, taking into account factors that can both increase and decrease risks.[30] The fact that certain risk factors may be present does not necessarily mean that a customer must be assigned to a higher risk category. For example, the sector in which a customer operates is only one of the factors the institution must consider in determining the customer risk classification[31]. The bank must take factors that increase, decrease and mitigate risks into account when conducting due diligence on an individual customer, while also making use of information obtained in the course of the customer relationship. This provides scope for differentiation in the application of measures to manage specific risks, depending on the customer's overall risk profile.

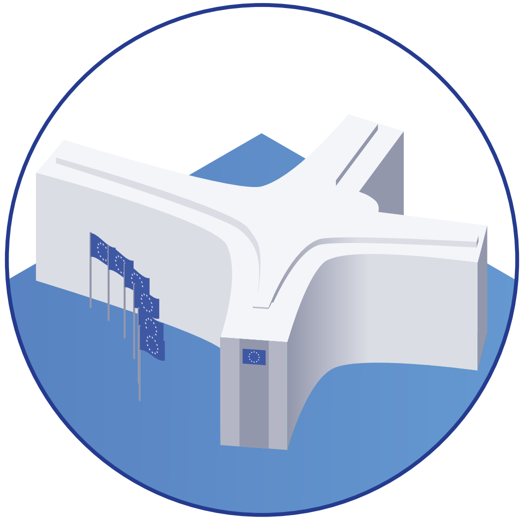
We will increasingly emphasise a risk-based approach in our policy communications and documents, and provide scope for innovative solutions. As mentioned, we support institutions by providing guidance on what we expect from them. Wherever possible, we will work with supervised institutions to analyse situations resulting in low or high risk, and investigate how confidence can be both given and obtained that the right measures are being taken for the risks identified. In doing so, scope will be available to apply innovative solutions, especially where these are more effective than traditional approaches (see also Section 4). In cases where banks have concerns about whether a particular approach is permissible, we will be happy to engage with them in dialogue. In some cases the law may not formally allow for the application of an innovative solution, even though such a solution may support the purpose of the law. In such cases we nevertheless intend to explore possibilities, for example by engaging with legislators on the removal of dispensable obstacles. The ultimate goal, after all, is to combat money laundering and terrorist financing as efficiently and effectively as possible.

Wherever possible, in addition to focusing on high-risk situations in our policy communications, we will also highlight low-risk situations and proportionate control measures. This is part of an evaluation cycle designed to assess the impact of policy statements and identity where they may need to be amended. Examples of potentially low risk situations to be discussed with the sector include:

- PEPs who make use of low-risk products.
- Foundations with limited annual turnover.
- A simple current account relationship with a private customer.
- Consumer credit and small loans.
- Private savings accounts without the possibility of cash deposits.

Technology and data are playing an increasingly important role in supervision.
In the *Supervisory Strategy 2021-2024*[32], we state that we consider data to be a crucial tool for effective and efficient supervision, and it is for this reason that our supervision is data-driven. The aim is to obtain a more complete picture of the risks institutions run. In the coming years, we also intend to increase the use of smart algorithms and artificial intelligence in our supervision. This naturally also applies to our integrity supervision. For example, our data science hub recently developed a transaction monitoring model to challenge banks' models.

[30] EBA Guidelines on ML/TF Risk Factors, Guideline 3.
[31] See: Further clarification of the questions about sectors in the annual integrity risk survey (dnb.nl).
[32] DNB, Supervisory Strategy 2021–2024.



3.4 European developments

A new European framework is under development for combating money laundering and terrorist financing. Although the Dutch supervisory legal framework is subject to significant international influence, and there is also much international cooperation, supervision remains a national matter. This will change down the road when the European Commission's AML/CFT package is implemented. The establishment of a new European supervisory authority, the Anti-Money Laundering Authority (AMLA), will give a more European character to supervisory activities aimed at preventing money laundering and terrorist financing (see Box 2).

Box 2 A new European framework for AML/CFT supervision

On 20 July 2021, the European Commission published a package of proposals to strengthen the common European approach to preventing and combating money laundering and terrorist financing. This package includes the following measures:

- The establishment of a European Anti-Money Laundering and Anti-Terrorist Financing (AMLA) Authority. Starting in 2026, this supervisory authority will directly supervise a number of selected institutions where European money laundering risks are high. It will also develop further regulations, and it will be a vehicle for closer cooperation between Member States.
- An Anti-Money Laundering Regulation (AMLR), which is also slated to come into force in 2026. The regulation unifies the rules that institutions must follow in order to prevent the misuse of the financial system for money laundering and terrorist financing, and will have direct operation in all Member States. The European rules will replace the Dutch Wwft in this area.
- A new Anti-Money Laundering Directive (AMLD6), which, among other things, will regulate the powers of national supervisors.

4 Use of data and technology

Technology can boost the effectiveness and efficiency of the fight against financial crime.[33] Dutch society and the Dutch economy are already highly digitised, which means that an excellent digital infrastructure is in place for the application of such technology. Combining human ingenuity with the power of big data and AI will enable financial institutions to prevent money laundering and terrorist financing more effectively and efficiently, while reducing the administrative burden on customers. We already see institutions experimenting with digital developments in customer due diligence and transaction monitoring. Provided the appropriate safeguards are in place, we support these activities.

For successful digital innovation, it is essential that institutions have the basics in order. In particular, this means having reliable *Wwft* compliance processes in place, and ensuring the quality and reliability of IT infrastructure and data, along with the availability of data. If these basics are not in order, then there is often little point in digitising processes. It is therefore essential that banks finalise the current remediation phase so that they will be able to effectively deploy innovative technology.

Using technology to combat financial crime can create tension with customer privacy safeguards (Box 3).[34] By their very nature, customer due diligence and transaction monitoring affect customers' privacy. Personal data is part of the information that institutions hold on their customers, which means that institutions have specific responsibilities with regard to safeguarding privacy. On the other hand, much of this data is necessary for institutions to comply with the obligations and expectations arising from the *Wwft*. When deploying digital technologies, it is therefore possible that *Wwft* compliance may require additional effort in the light of GDPR provisions. The "traditional" approach to fighting crime reveals that a solid legal basis and appropriate accountability measures can alleviate this tension.

[33] M.V. Achim, S.N. Borlea & V.L. Vaidean (2021), Does technology matter for combating economic and financial crime? A panel data study, Technological and Economic Development of Economy, 27, 1, p. 223-261.
[34] FATF (2017), FATF Guidance - Private Sector Information Sharing.

Box 3 Recommendations on privacy safeguards

The Dutch Data Protection Authority (AP) states in its advisory opinion of November 2021 on the amended proposal for the Data Processing by Partnerships Act (*Wet Gegevensverwerking door Samenwerkingsverbanden - WGS) that: "...preventing and combating serious and subversive crime is of such importance that it is clear, also to the AP, that this may require significant infringements of the fundamental right to the protection of personal data."* However, the AP considers further amendments to the bill necessary to prevent the erosion of principles it applies in its assessments, such as the presumption of innocence and the principle of data minimisation. In the opinion of the AP, the bill goes further than strictly necessary, contains insufficiently clear and precise rules and inadequate procedural and material safeguards. In the AP's view, the bill therefore does not meet the proportionality test. Necessary adjustments identified by the AP include better justification of the need for specific partnerships, deletion of secondary objectives of the law, specification of risks, and inclusion of clear rules on when partnerships may take action and on the exceptions to the rights of data subjects that the law allows.

In a reaction to this recommendation and other input, the Minister of Justice and Security stated in December 2021 that he was strengthened in his conviction that the bill could responsibly steer joint data processing by partnerships in a sound and lawful direction. However, a number of concerns would still need to be addressed by amending the law as soon as it is adopted along with additional regulation of a number of topics in a general administrative order.

Similar advisory opinions have been issued regarding the Action Plan on Money Laundering Act. In an opinion on this bill from January 2021, the Council of State points out that exchanging information as part of the joint monitoring of bank transactions and in customer due diligence can lead to far-reaching infringements of fundamental rights. As part of its opinion, the Council does endorse the importance of tackling money laundering and it recognises the relevance of the gatekeeper role of financial institutions. Due to the concerns, the Council has advised against submitting the bill in its current form to the House of Representatives. The AP advised along the same lines on this bill in March 2020.

There is also criticism of the upcoming European anti-money laundering and anti-terrorist financing bills (see Box 2). The European Data Protection Board (EDPB) and its members (including the AP) wrote to the European Commission in May 2021 and May 2022, stating that the current proposals represent a far-reaching and disproportionate infringement of customer privacy. According to the EDPB, adjustments are needed to ensure consistency with the GDPR and to avoid legal uncertainty.

4.1 Smarter customer due diligence

Greater digitalisation can increase the effectiveness and efficiency of know-your-customer (KYC) processes. Due diligence can be time-consuming and labour-intensive for institutions and customers. Digitalisation can offer a solution. The successful digitalisation of KYC processes depends on high-quality and complete datasets and reliable models that can assess customer risks on the basis of this data. Both of these points are discussed in more detail below, taking a specific technological innovation as an example.

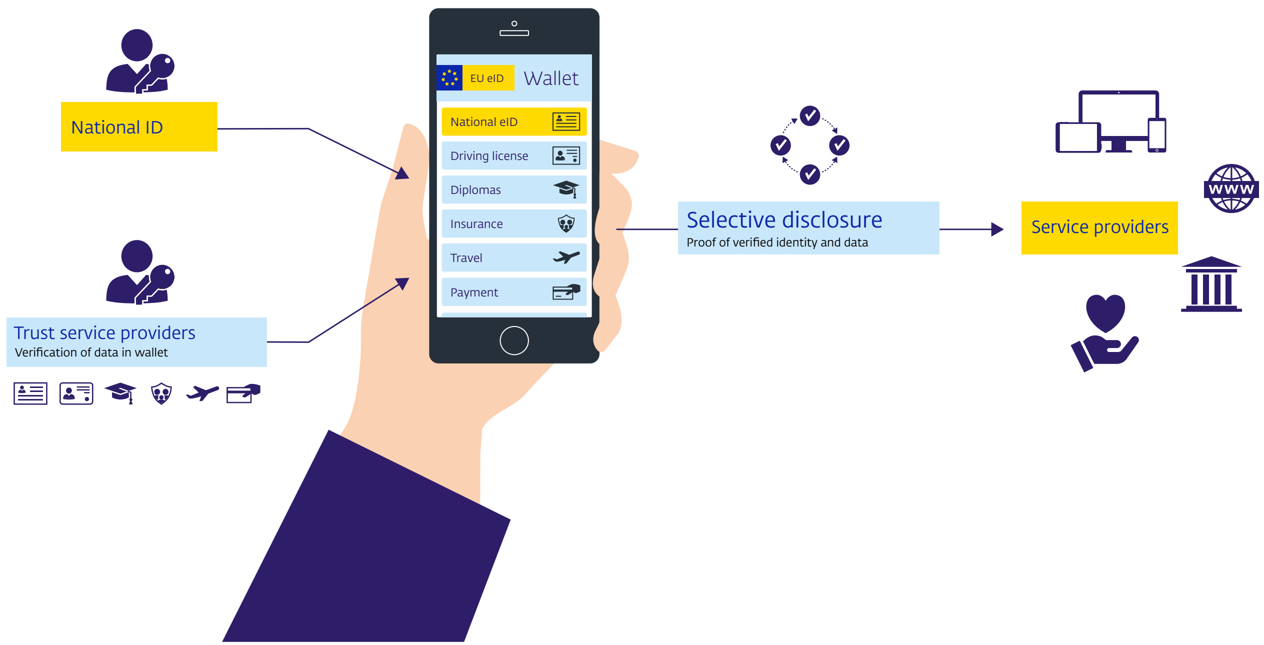
4.1.1 Access to data: digital identity and wallet (eID)

A digital identity can dramatically simplify identification and verification in customer due diligence processes, thereby reducing the administrative burden on the institution and the customer. A central component of customer due diligence is the identification[35] of the customer and the verification of this identity. Currently, institutions often request the data required for this identification from the customer in a separate process. A digital identity can simplify these steps. In June 2021, the European Commission put forward a proposal on the revision of the European eIDAS regulation,[36] which provides for a digital identity for EU citizens. It is expected that the revised regulation will be in place beyond the end of 2022. The Commission aims for 80% of EU citizens to

[35] The following are required for identification: legal name, address, citizen service number and date of birth.
[36] A trusted and secure European e-ID - Regulation | Shaping Europe's digital future (europa.eu). See also Electronic Identities And Trust Services, Everything you need to know about eIDAS | Online access to public services in the European Economic Area (eIDAS) | Rijksoverheid.nl.

make use of this technological innovation by 2030.[37] This eID will take the form of a "wallet", in which other data can also be verified and shared such as diplomas, address details, medical data and authorisations (of legal entities) (Figure 8). Such data will only be included in the wallet if it comes from a reliable and independent source - for example from a university in the case of a diploma. Individuals can use the eID wallet to identify themselves and choose which personal data to share, both online and offline. This is a simple and secure way for institutions to request information from customers, and for customers to share information. The system has the potential to boost the reliability of identification and verification and to reduce the administrative burden on both customer and bank. It goes without saying that a customer must consent to the sharing of all or part of the data stored in their eID wallet.

Figure 8 European eID wallet



4.1.2 Using artificial intelligence in customer risk analysis

Data analysis using artificial intelligence can – if adequate safeguards are in place – take customer risk analysis to a higher level. Research by McKinsey at various financial institutions in 2019 reveals that customer risk classification is often unreliable: low-risk customers are often classified as high-risk (false positives).[38] This places an unreasonable burden on the institution and the customer, as additional due diligence must be carried out unnecessarily. A more accurate analysis would therefore significantly reduce the administrative burden on both the institution and the customer. It is also possible that customers may be classified as low risk, while they are in fact high risk (false negative). This is particularly problematic because low-risk customers are seldom if ever reviewed, which means that potentially criminal practices can remain undetected for quite some time in some cases. According to the European Banking Authority (EBA)[39], improved models based on artificial intelligence and using machine learning have the potential to identify suspicious actors and activities with greater accuracy. Machine learning is a type of artificial intelligence that introduces self-learning components into models. The outcomes of the model are compared to the programmed objective, creating a feedback loop of how well the outcome meets the

[37] European Parliamentary Research Service (2022), Revision of the eIDAS Regulation: Findings on its implementation and application.
[38] McKinsey & Company (2019), Transforming approaches to AML and financial crime.
[39] EBA (2020), Report on Big Data and Advanced Analytics, p.20.

objective. This means that the outcomes of the model are not explicitly programmed, but that the model itself must learn to arrive at these outcomes. This process ensures accurate analysis while reducing false positives and false negatives. For machine learning to work, however, the dataset must be of good quality and complete. Models must also be capable of learning from successful or unsuccessful outcomes. Feedback from FIU-NL and investigative authorities on reported unusual transactions can be beneficial to this learning process.

Appropriate safeguards are indispensable for the further deployment of AI. It is essential to retain human involvement in order to prevent AI from functioning as a kind of black box whose results are not easily traceable.[40] Potential bias in the models must also be kept in mind[41] along with the degree of explainability of a specific risk profile as an outcome for a customer.[42] This is essential because of the major impact gaining and retaining access to financial services can have on customers. The AI process and the resulting analyses must also be transparent for the supervisory authority. Institutions must therefore diligently structure their AI governance, for example by assigning authority for the deployment of responsible AI within the usual three lines of defence.

4.2 Smarter transaction monitoring

Machine learning can also improve transaction monitoring. Banks deploy transaction monitoring systems on a large scale to detect anomalous transactions.[43] Although some banks are experimenting with more advanced models, these currently tend to be relatively static rule-based systems. The predictive ability of these systems is relatively limited, meaning they also produce many false positives and false negatives. Rule-based systems rely on threshold values (e.g. a quantity of cash deposits) for certain criteria. When these are exceeded, the system automatically designates a transaction as anomalous. According to the EBA[44], using machine learning for this purpose would result in improved transaction analyses, thus increasing the effectiveness of transaction monitoring and reducing the burden on customers and institutions. Moreover, these models are better able to cope with a more dynamic environment in which the financial system is in an ongoing state of development while also facing a constant barrage of threats. Self-learning components can help keep transaction monitoring systems up-to-date on a real-time basis.

4.2.1 Ex ante transaction monitoring

Improved predictions from transaction monitoring systems enable institutions to stop and analyse anomalous transactions before they are executed. In the end, an ounce of prevention is worth a pound of cure. This is why banks use models to assess transactions before executing them. If a transaction is deemed highly unusual, the bank may decide to suspend the transaction while an analyst scrutinises it. Unusual and suspicious transactions can thus be stopped at an early stage. Institutions already use ex ante transaction monitoring to stop certain transactions, for example when implementing sanctions. Rule-based methods are probably not accurate enough to do this on a larger scale, however. Machine learning will likely prove beneficial in this respect. However, it is important that clear arrangements are made about two things: 1) the limits that must be exceeded before institutions can stop transactions; 2) human intervention is always required – the "system" cannot definitively stop transactions automatically.

[40] WRR (2021), Opgave AI. De nieuwe systeeemtechnologie (Mission AI. The new system technology).
[41] J. Yong & J. Prenio (2021), Humans keeping AI in check – emerging regulatory expectations in the financial sector, FSI Insights No 35.
[42] EBA (2020), Report on Big Data and Advanced Analytics.
[43] E. Bosma (2022), Banks as Security Actors: Countering Terrorist Financing at the Human-Technology Interface.
[44] EBA 2020, Report on Big Data and Advanced Analytics, p. 23.

4.2.2 Explainable AI in transaction monitoring

One challenge of using machine learning models is that they can be difficult to explain. This may affect the extent to which the outcomes of these models can be used. Indeed, if a customer's transactions are investigated and possibly reported to FIU-NL based on detection by a machine learning algorithm, an institution must be able to explain the model and justify why the transactions in question are unusual. Justifying the report by blaming the system ("computer says no") is not a good enough reason to investigate. However, this does not mean that institutions cannot use these more complex forms of AI. This is the reason for the essential precondition prohibiting automatic decision-making by the systems. Analysts can then use the models to support them in their work. In addition, complex systems can be used in combination with complementary explainability tools, which provide insights into how the model works.[45]

4.3 Using network analyses

Network analyses examine the connections between entities in order to better understand their relationships. Network analyses complement existing machine learning applications. Network analyses of each individual customer can be used as input to boost the accuracy of transaction monitoring models. Instead of analysing an individual, a network (or component of a network) is examined for known methods of money laundering and other atypical consumer behaviour. Networks are formed by relationships between customers and related activities. These links may be based on internal data such as transfers or shared property, or on external data such as shared addresses or use of the same ATM. Banks recently used this method to roll up an underground banking network consisting of 200 suspects. The underground banking risk indicators from this discovery were subsequently incorporated into new models, significantly increasing the predictive value of the models.

4.4 Data issues

Digital innovation depends on high-quality and complete data. When using machine learning, the maxim of "garbage in, garbage out" applies. If the data is of poor quality, the results will be too, no matter how good the models themselves are.[46] For example, automatic customer screening against terrorism lists (list matching) is of little use if names are not spelled correctly or consistently. Data is of poor quality if it is inconsistent, incomplete or duplicated. Data collection methods, database architecture and ensuring data integrity are all important components to ensure data quality.

Sharing relevant data between different parties is a core element in combating financial crime. Analysing data from different sources has many advantages, as combining datasets leads to new insights as well as to better decision-making, more thorough research and more robust products and services. However, datasets from different sources cannot simply be combined, partly due to GDPR provisions. Nevertheless, technology does make it possible for different institutions to share data without actually divulging sensitive information. One example of this is Secure Multi-Party Computation, as described by research organisation TNO (Box 4). Banks, in cooperation with TNO, have already successfully used this method in the joint detection of fraud.[47]

[45] EIOPA (2021), Artificial Intelligence governance principles: towards ethical and trustworthy Artificial Intelligence in the European insurance sector.
[46] Bain & Company (2018), How Banks Can Excel in Financial Crimes Compliance.
[47] A. Sangers et al. (2019), Secure Multiparty PageRank Algorithm for Collaborative Fraud Detection, in: Financial Cryptography and Data Security, p. 605-623.

Box 4 Secure Multi-Party Computation (MPC)

Secure MPC is an innovative solution to provide the functionality of a shared database in which different parties provide data, but without the data being visible to others. MPC is a collection of cryptographic techniques that allow multiple parties to perform computations on data in unison. Because the data is protected by cryptography, it can be analysed without the parties ever being able to see other others' data.

Appropriate legal bases are necessary for data sharing between parties. The Data Processing by Partnerships Act (WGS) is an example of such a basis. The WGS provides a legal basis for systematically sharing and processing personal data for purposes of substantial public interest. Both administrative bodies and private parties may participate in these partnerships. The proposal was adopted by the House of Representatives at the end of 2020 and is currently before the Senate. In the coalition agreement, the parties indicated their desire to anchor the basis for data exchange in legislation with appropriate safeguards.

5 Effective thanks to cooperation

5.1 Cooperation in the Netherlands

Effectively preventing and combating money laundering and terrorist financing is only possible if parties work together.[48] A large number of parties are involved in preventing and combating these illicit practices (see also Section 1), each with their own mandate and responsibility. The FATF sees cooperation as a strength of the Dutch anti-money laundering and anti-terrorist financing policy. Leveraging synergies for the best possible result requires setting shared goals and priorities. This does not diminish the individual responsibility of each of the parties. Cooperation between partners is not a substitute for individual roles and responsibilities. Rather, it represents a strengthening of everyone's role and responsibility in contributing to the shared goal of preventing and combating the misuse of the financial system for the purpose of money laundering or terrorist financing. When performing its task in the chain, each party always keeps the ultimate goal in mind.

There is great societal urgency to actively prevent and combat financial crime. The coalition agreement calls for intensifying efforts to hunt down criminal money and prioritise financial investigations and intelligence to disrupt illicit money flows. This is increasingly taking place through cooperation between public parties, in public-private partnerships and between private parties. Money laundering and terrorist financing are pre-eminently international phenomena, meaning it is also essential to strengthen international cooperation to prevent and combat these activities.

Public cooperation

The Financial Expertise Centre (FEC) is the forum for public-sector cooperation. The FEC is a partnership between authorities with a supervisory, monitoring, prosecution or investigative task in the financial sector. The centre was established to strengthen the integrity of this sector. Partners in the FEC exchange insights, knowledge and skills with the aim of taking a joint, more problem-focused approach to reducing flows of criminal money, all based on more robust and reliable information. Public-public cooperation takes place, for example, in the joint activities of the FEC partners to combat terrorist financing. This includes investigating foreign financing of non-profit organisations for possible links to terrorism.

[48] See also the Plan van aanpak witwassen (Plan of Action on Money Laundering) (currently only available in Dutch) by the Minister of Finance and the Minister of Justice and Security, 30 June 2019, and the recommendations in: Society and Security Foundation (Stichting Maatschappij en Veiligheid) (2022), Poortwachters tegen witwassen (Gatekeepers against money laundering) (currently only available in Dutch).

Public-private partnerships

Alongside cooperation in the public domain, the public-private partnership (PPP) is also an important function of the FEC. The members of this partnership are the regular public partners, the four major banks and the Dutch Banking Association (NVB). The FEC's PPP also focuses on information exchange, sharing knowledge and joint projects. An example of an effective public-private partnership initiative is the Serious Crime Task Force, in which the police, the Public Prosecution Service, FIU-NL and the FIOD work together with a number of large banks to tackle subversive crime. In addition, FIU-NL and the banks exchange knowledge in the Fintell Alliance in order to improve banks' transaction monitoring and analyses, which in turn will lead to more reliable reports.

We see clear added value in public-private partnerships. We therefore welcome our participation in public-private initiatives,[49] in which we endeavour to take on a driving, advisory or catalysing role. We are also receptive to participating more actively in specific collaborative projects, provided that these are in keeping with our supervisory task. In doing so, we will consider whether participation contributes to the supervisory objective of preventing financial crime. Participation in a collaborative project must be appropriate to our powers and obligations as a supervisory authority, and we must have the resources available.

Cooperation between private parties

One initiative in the field of private-private partnerships is the collaboration between five Dutch banks under the name Transaction Monitoring Netherlands (TMNL). The banks work together to monitor transactions for signals that may indicate money laundering and terrorist financing. We are not a partner in this project, but we do support it and we contribute where possible by sharing our insights. This collaborative project provides added value by combining transaction data from different banks. This allows for the identification of patterns and connections that would be impossible for a single bank on its own. TMNL can thus become a mechanism for "smarter transaction monitoring" (see Section 5.2). This does require the inclusion of appropriate privacy safeguards for processing personal data in accordance with the GDPR. It would also be beneficial if institutions were allowed to outsource transaction monitoring while retaining responsibility. Section 10 of the *Wwft* currently prohibits this, however. Amending this provision is part of the Plan of Action on Money Laundering. TMNL can potentially be expanded to include other banks or non-bank partners. Establishing a feedback loop with FIU-NL would also boost effectiveness. In such a loop, FIU-NL would provide feedback on the rate of successful detection based on TMNL analyses.

International cooperation

We welcome closer European cooperation. As discussed in Section 3, supervisory activities aimed at preventing money laundering and terrorist financing are slated to become more European in nature. We see the implementation of the European Commission's proposals as essential for achieving a more coordinated and uniform approach to preventing and combating money laundering and terrorist financing. We also see scope for a phased growth model for the new European authority (AMLA), in which more and more institutions can gradually fall under direct European AML/CFT supervision. Comparable to the European Commission's proposal, we would like to expand the involvement of national supervisory authorities in the European decision-making process and in other areas.

[49] DNB (2020), DNB als partner in publiek-private samenwerking tegen financieel-economische criminaliteit (DNB as a partner in public-private partnerships against financial crime) (currently only available in Dutch).

5.2 Future prospects

Far-reaching cooperation between public and private parties makes preventing and combating financial crime more effective. Such partnerships boost the overall level of knowledge and bring the risks, trends, typologies and indicators related to financial crime into sharper focus. Additionally, information and signals can be shared by partners in the chain with the aim of combating crime and ensuring robust supervision along with effective investigations and prosecution. Scope remains for enhancing public-private partnerships, for example with regard to coordinating the approach to financial crime in the Netherlands. Issues must be prioritised prior to jointly tackling them to ensure staffing levels and other resources are up to the task and to provide legal opportunities to exchange information.

Efforts to improve coordination in tackling financial crime in the financial sector would benefit from centralised control and overriding power to tackle money laundering and terrorist financing more effectively and efficiently. The FEC can play an important role in coordinating these efforts. In this capacity, the FEC will be empowered to keep the purpose of the *Wwft* and the objective of cooperation in the chain clearly in mind. This can serve as the basis for formulating concrete and measurable operational objectives and initiating projects. The following preconditions, which are explained below, are important in this regard: strict prioritisation, sufficient capacity and exchange of information.

Strict prioritisation is needed to identify issues that can be tackled jointly. Money laundering and terrorist financing can be tackled jointly in many areas, and it is wise to make choices based on consensus. Focusing on a number of priority topics will make public-private partnerships even more effective. The National Risk Assessments (NRAs) for money laundering and terrorist financing can be used as guidelines to prioritise issues for a subsequent joint effort.

Effective cooperation requires sufficient capacity. Each link in the chain must have adequate capacity to execute its tasks. Indeed, the link with the least capacity will form a bottleneck for the entire chain. In 2021, the four major banks in the Netherlands alone devoted 10,000 FTEs of staffing capacity to preventing money laundering and terrorist financing (see Section 2). This capacity has grown significantly in recent years, partly due to ongoing remediation processes at various banks. Sufficient capacity is also essential for the public partners in the chain. FIU-NL, the Fiscal Intelligence and Investigation Service and the Public Prosecution Service have received additional financial resources from the Ministry of Justice and Security specifically to combat subversive crime. In the Action Plan on Money Laundering, the Minister of Finance states that capacity for supervising *Wwft* compliance remains a concern because of the importance of exercising assiduous risk-based supervision by the competent authorities.

The chain for reporting and investigating unusual transactions can be made more effective. Legislation could be changed, whereby institutions are no longer required to report “unusual” transactions, but rather to focus on reporting “suspicious” transactions, i.e. if the institution has reasonable grounds to suspect that the customer’s actions are related to money laundering or terrorist financing.[50] Transaction monitoring systems could then be fine-tuned, reports would be of better quality and their numbers would decrease. FIU-NL would get a more focused data set, which would foster an effective take-up further down the chain. This would also allow the Netherlands to deviate less from the international practice of primarily reporting suspicious transactions. As discussed in Section 4, machine learning can help make this a reality. More possibilities for data sharing within the reporting chain and the feedback loops discussed above will also boost effectiveness.

[50] This does not diminish the requirement to refrain from executing transactions which are known or suspected to be linked to proceeds from criminal activity or to terrorist financing.

Information exchange is essential for both the public and private parties when it comes to preventing and combating financial crime. The saying “two know more than one” also applies to the public parties in the chain. By sharing information about specific cases or phenomena, each party can perform its public duty more effectively and based on more complete insights. This must, of course, be done diligently and with an emphasis on confidentiality and privacy. This kind of information exchange will help prevent and combat financial crime. Private parties, in turn, have access to information that is relevant for fulfilling their own roles and responsibilities. In addition, private parties are able to detect anomalous behaviour, which makes it possible to intervene at an early stage in the case of criminal activity. Private parties thus have information at their disposal that would be useful to public parties. The reverse is also true, however. It is therefore important for public and private parties to ensure the thorough and appropriate exchange of information. The chain for reporting and investigating unusual transactions can thus be made more effective. The Action Plan on Money Laundering states that the Minister of Finance and the Minister of Justice and Security recognise the importance of information exchange for the effective fulfilment of the tasks of the public chain partners and of the gatekeeper role. This has been formulated in the legislative proposal for the plan to tackle money laundering and the proposal for the Data Processing by Partnerships Act (see Section 4).

Authors: Hans Brits, Frans van Bruggen, Charlotte Dijkstra, Richard Hoff,
David Keijzer, Joris van Toor, Lisanne Veldhuis.

We thank all external and internal stakeholders who contributed to the drafting of this report.