Digital redaction (14-7-24) to adapt
For typo's/misunderstanding

European Commission
Directorate-General for Justice and Consumers
Deputy Director-General
Rule of Law, Fundamental Rights and Democracy (JUST.C)
[redacted]
1049 – Brussels
Belgium

Ir. Simon Lelieveldt as an
consumer and professional
[redacted]

Mr Lelieveldt as chair of the
Foundation on
Human Rights in Finance.EU
(legal@hrif.eu)

PO Box 15673
1001 ND Amsterdam

July 12, 2024
Amsterdam

Re: Formal request to take up human rights evaluation and evaluation AMLD5

Dear [redacted]

From the EU website I have concluded that you may well be in charge of discussions on the Rule of Law in Europa and the safeguards and procedures that need to be in place to respect human rights, as a part of the values of the European Union. Trickling down from the International Declaration of human rights, the European Convention on Human Rights as well as the Charter of Fundamental Rights (based on the Treaty of Lisbon) safeguard very important human rights in Europe.

In this letter I formulate two formal requests to the European Commission in three capacities: first of all as an individual person whose rights have been violated for over three years now. Second: as a compliance professional in the financial industry that needs to reconcile incompatible legislative acts. And third I am adressing the European Commission as the chair of Human Rights in Finance.EU, a civil society organisation that seeks to prevent human rights violations occuring due to a lack of respect of the three lawmaking institutions for human rights/fundamental rights.

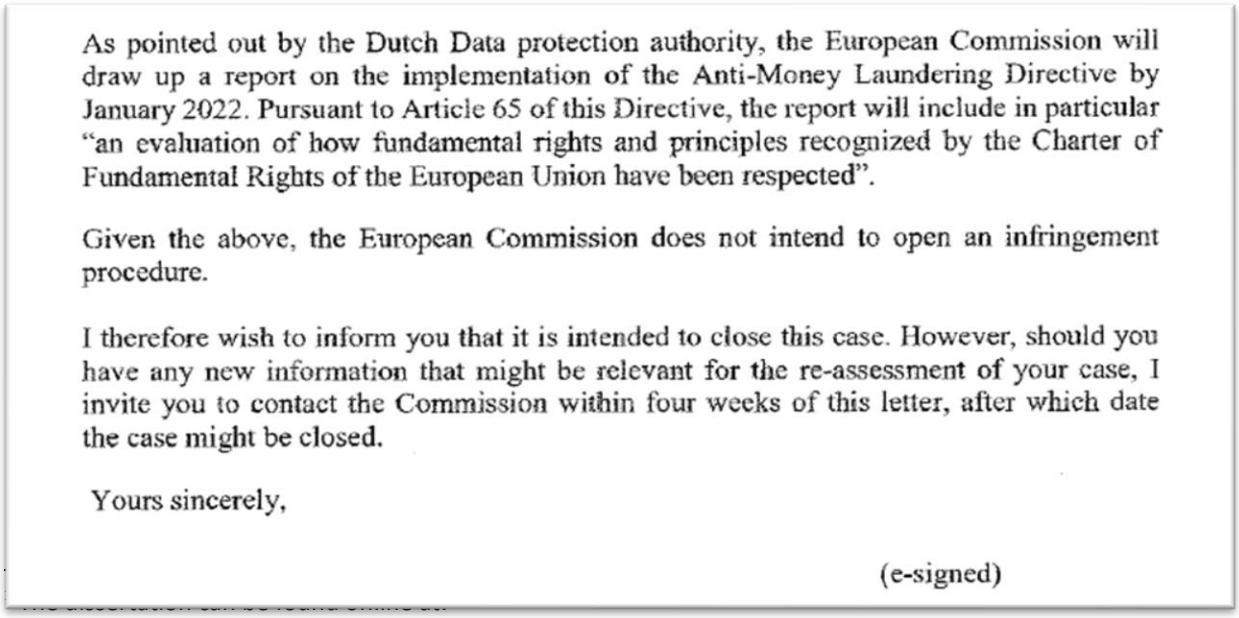
Digital redaction (14-7-24) to adapt
For typo's/misunderstanding

Particularly in the financial sector the right to privacy, the right to a fair trial, the innocence presumption, the right to property, the right to not be discriminated/profiled and the right to access to health care, universal services (via a the right to a bank account) are violated due to the excessive regulations and policy inititiaves initiated and driven by the European Commission anti-money laundering and financial services directorate FISMA. This is of **individual concern** to me as a citizen, professional and to HRIF.EU as a human rights defending organisation.

1. Infringement not opened because: a human rights evaluation would occur
Over the years 2019 and 2020 I have, both in my personal and professional role, sent in two infringement complaints, outlining the incompatibility of the rules of the fifth anti-money laundering directive with the human rights safeguards in the Treaties of Rome and Lisbon and requesting the Commission to investigate the infringements that the AMLD-rules form on the Human Rights of citizens in Europe.

In my complaints (15-11-2019, CHAP(2019)03200 and 21 May 2020, CHAP (2020)/01471) I referred to the 600plus page dissertation of Carolin Kaiser, Privacy and Identity Issues in Financial Transactions, from 2018. This dissertation outlines that, considering the prior rulings of the Court of Justice with respect to Digital Rights Ireland, the Data Retention directive, the AMLD-rules in Europe could also well be annuled as they constitute a range of infringements of human rights.[1]

The Commission services replied by letter of October 25, 2020, that it did not intend to open an infringement procedure and for its arguments it referred to the upcoming evaluation of human rights, required under article 65g of the AMLD5. Although I did not like that answer (and later lawsuits in the Netherlands proved the validity of my complaint with a judge annulling Dutch law as contrary to the EU rules), I did accept the argument and expected the Commission to live up to its duties in this respect.



As pointed out by the Dutch Data protection authority, the European Commission will draw up a report on the implementation of the Anti-Money Laundering Directive by January 2022. Pursuant to Article 65 of this Directive, the report will include in particular "an evaluation of how fundamental rights and principles recognized by the Charter of Fundamental Rights of the European Union have been respected".

Given the above, the European Commission does not intend to open an infringement procedure.

I therefore wish to inform you that it is intended to close this case. However, should you have any new information that might be relevant for the re-assessment of your case, I invite you to contact the Commission within four weeks of this letter, after which date the case might be closed.

Yours sincerely,

(e-signed)

[1] The dissertation can be found online at:
https://pure.rug.nl/ws/portalfiles/portal/65647303/Complete_thesis.pdf

Digital redaction (14-7-24) to adapt
For typo's/misunderstanding

2. Infringement complaint sent in by Human Rights in Finance.EU

On 12 October 2023, the foundation Human Rights in Finance.EU filed an infringement complaint again, given that the Dutch government continued infringements of Human Rights by sticking to excessive regulation on acces to markets as well as on unusual transactions including the failure to act to stop a joint transaction monitoring company of banks (that acted without legal title).

The complaint was registered: CPLT(2023)02904 and our request to have DG JUST staff included in a meeting to explain our complaint was denied by FISMA. We then re-iterated in an e-mail of January 18, 2024, our request to have someone from DG JUST present. In this repeated request we reffered to the prior infringement procedures and the fact that it appeared as if new legislation was being drafted/finalised without the human rights evaluation ever having occurred:

> While we understand the Commission's workload and acknowledge the desire to push forward new legislation, we are concerned about the apparent delay and current absence in assessing the human rights implications of the AMLD directive under Article 65g of Directive 2018/843. This issue, coupled with the impending AML-regulation, is of significant concern as it potentially infringes upon the rights of EU citizens and companies, subjecting them to what we perceive as unconstitutional mass surveillance.
>
> It is not our intention to cast doubt on the Commission's commitment to upholding human rights. However, given the gravity of the situation, we believe it is crucial to emphasize the potential legal ramifications of a failure to act in accordance with EU treaties and agreements on human rights. As responsible stakeholders, we are compelled to express our reservations and concerns about the Commission's responsibilities and potential liability for damages that may arise from a failure to uphold the spirit of these agreements.

In response FISMA was not willing to change the delegation and we had a constructive online meeting on January 25, 2024. In the meeting we promised to provide further documentation on matters of conern in the Netherlands, relating to the investigation of unusual transactions and unlawful actions of government and private players which are in violation with the GDPR, Human Rights.

Over the course of a couple of months HRIF.EU has via e-mail informed DG FISMA that it had sent an enforcement request to the Dutch central bank to ensure that banks would stop their collective transaction monitoring business in the Netherlands, which is a violation of both article 10 of the Anti-money laundering law, article 6 of the GDPR (lack of title), article 9 of GDPR (processing of sensitive personal data without formal legal title in law) as well as Dutch penal law code article 138c (unlawful copying and storying of personal information).

We have repeatedly asked the European Commission to intervene in this matter and take up the infringement. While we still have the sending of some additional information on our to-do list, the lack of response to our e-mails and the information sent is concerning. We presented a legal opinion clarifying the criminality of banks joint transaction monitoring (and intrusion of privacy) and received no response.

Digital redaction (14-7-24) to adapt
For typo's/misunderstanding

Of course we understand that there can be a difference of appreciation between striking the balance in terms of protection of privacy, fundamental rights and the duty of governments to ensure society is safe. However, the lack of any communication on the matter meant that we had to legally hold the European Commission liable and accountable as it hasn't acted/responded at all to our calls to immediately ensure the local Dutch infringements of human rights and the GDPR violations come to an end.

Our e-mail of June 20, 2024 thus explained how we sent our legal opinion on the criminality of banks behaviour to private actor Amazon Cloud Services but also requested the commission to act, while reserving all rights:

> In a legal sense we cannot escape the legal reality and must also hold the European Commission liable and accountable for letting this massive cybercrime (and privacy infringement) continue despite having knowledge of the illegality of it.
>
> In a similar vein we need to reserve all rights for further actions and compensation claims on behalf of the data subjects, as the violation has been ongoing for 3 years now and covers all citizens and companies of NL, except the multinational companies.

Due to the pressure exerted by our foundation and the publication of investigative journalist Strop at the website Follow the Money ('Bank's are spying on everyone's data, but no one intervenes'). the 5 Dutch banks and the transaction monitoring company finally decided to consider stopping transaction monitoring Netherlands in the fall. It is unclear if this will truly happen. Fact remains that since March 2021, approximately over 12 billion transaction records with personal data have been processed and profiled without legal title, constituting a criminal act under Dutch law. Both the Ministry of Finance in the Netherlands, the Dutch Central Bank and the European Commission were fully aware of this, given that the monitoring initiative was also presented in the FATF-evaluation on the Netherlands.

3. Root cause of the problem: failures to legislate according to agreed rules

It is my personal and professional opinion as well as the opinion of the foundation HRIF.EU that the root cause of this massive privacy infringement is due to a lack of respect by EU institutions for the rules that they drafted themselves with respect to careful and better regulation and evaluation of human rights.

We point out that the Interinstitutional Agreement of 13 April 2016 on Better Law-Making stipulates in article 25:

> The Commission shall also explain in its explanatory memoranda how the measures proposed are justified in the light of the principles of subsidiarity and proportionality and how they are compatible with fundamental rights. The Commission shall, in addition, give an account of both the scope and the results of any public and stakeholder consultation, impact assessment and ex-post evaluation of existing legislation that it has undertaken.

Digital redaction (14-7-24) to adapt
For typo's/misunderstanding

In addition article 25 stipulates:

> The Commission shall continue to fully play its institutional role to ensure that the Treaties and the case-law of the Court of Justice of the European Union are respected.

We point out that article 65 of the 5th Anti Money Laundering directive stipulates:

> 1. By 11 January 2022, and every three years thereafter, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and to the Council.
>
> That report shall include in particular:
> (g) an evaluation of how fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union have been respected.

4. Shortcomings with respect to the AML-package

When looking at the actual state of affairs we noted that the impact assessment of the the AML-Package has a range of shortcomings and the promised human rights evaluation under AMLD5 article 65g has never been made and the specific rules as to REFIT/Recast procedures have been abused in order to speedily adopt new rules, rather than first evaluate the old rules, evaluate human rights impacts and then draw up new rulees.

> **8 REFIT (SIMPLIFICATION AND IMPROVED EFFICIENCY)**
>
> No evaluation of the existing AML Directive has taken place to date prior to the preparation of the present impact assessment (see annex 4). The transposition deadline of the fourth AMLD was June 2017, and the transposition deadline of the fifth AMLD was January 2020. In both cases a number of Member States did not transpose on time and infringement proceedings were launched. The assessment of completeness and conformity of transposition by the Commission is still ongoing for both Directives. Article 65 of the consolidated AML Directive requires the Commission, by 11 January 2022 and every three years thereafter, to submit a report on the implementation of the Directive in the Member States. However, given transposition delays, there is not yet a series of three years of data on implementation of the fourth AMLD, much less the fifth.
>
> The reasons behind the urgency of the AML Action Plan of May 2020, and of the legislative package accompanied by this impact assessment, before evaluation of the existing AML Directive, are explained in the Introduction and in Annex IV. The primary objective of the present proposals is to increase the effectiveness of the EU AML/CFT regime, with the aim of reducing the amount of criminal ML/FT in the European Union, rather than simplification and improved efficiency.

The lack of due care for legislation impacts all the rules of the AML Package which are: Regulation 2023/1113 (fast tracked travel rule), Regulation (EU) 2024/1620), Regulation (EU) 2024/1624 and Directive (EU) 2024/1640). All these rules can be assumed to have fundamental flaws and lack of balanced weighing of human rights principles.

Digital redaction (14-7-24) to adapt
For typo's/misunderstanding

5. Request on Commission position

We notice that the Comission has failed to act (and hold the Commission responsible and liable) as listed below under 1-4. And we formally request the Commission to 1): make up for those failures immediately and 2): communicate its position on:

1 – the missing evaluation of human rights impact of the AMLD5 legislation as to be published by January 2022; when will it be executed?

2 – the commitment of the Commission to fully play its institutional role to ensure that the Treaties and the case-law of the Court of Justice of the European Union are respected; our request: when and how will the Commission validate the legality of the rules in the AMLD Package against the Prokurat Verdict and other relevant verdicts of the Court of Justice and Human Rights Court?

3- the lack to execute a prior evaluation of the functioning of the AMLD5 directive before putting in place the AML Package – considering the best practices in EU regulation as well as the expectations to be derived from the Better Law Making agreement

4- the lack to demonstrate for each of the human rights (privacy, innocence presumption, right to property) infringing rules in the regulations of the AML Packages, the compatibility with human rights, on a per measure basis, as to be expected as best practice, as a reflection of the values of the EU and the constitutional norms of Member States and under the Better Law Making Agreement.

Even though the package may now be published in the Official Journal, we are convinced that the lack of action of the Commission needs correction. When later evaluations by the Commission demonstrate the incompatibility of some of the rules with fundamental rights, the Commission can take corrective action itself and pro-actively. Alternatively, if the Commission does not want to correct itself, it should at least be held to execute the obliged evaluations and assessments in order for citizens, companies or NGO's like HRIF.EU to take up law suits and address the shortcomings via the courts.

We stand ready to further explain our request and look forward to your response and the Commission position on this matter. To demonstrate the relevance of this matter, we have attached the previously mentioned legal opinion on the criminality of excessive transaction monitoring by banks which happened in the Netherlands for 3 years.

With kind regards

Simon Lelieveldt	Simon Lelieveldt	Simon Lelieveldt
As a person	Chairman Human Rights in Finance.EU	Professional

VIA MAIL AND E-MAIL TO: abuse@amazonaws.com
Amazon Web Services EMEA SARL
[redacted]
vice president of Sovereign Cloud at AWS
38 Avenue John F. Kennedy,
L-1855, Luxembourg

Human Rights in Finance.EU
PO Box 15673
1001 ND Amsterdam
legal@hrif.eu

June 20, 2024

Subject: Information on criminality and unlawful data processing by Transaction Monitoring Netherlands and Dutch banks – urgent request to end servicing TMNL and PLC-infringements and GDPR-violations of AWS by the end of June 2024

Dear Mr [redacted] staff at AWS,

As we understand from public sources, the Dutch company Transaction Monitoring Systems Netherlands is one of the AWS-customers (we assume that they transact with Amazon Web Services EMEA SARL). TMNL is, under the AWS service agreement due to comply with article 1.11 of the AWS-service terms: ensuring that personal data is processed under legal title.

With the attached legal opinion, we inform you that the legal basis of the business operations and data processing of TMNL is missing and in fact their operations, which encompass the processing and full surveillance of 4 billion records Dutch citizens/companies (including US citizens and companies) are a violation of Dutch Anti Money Laundering Law (article 10 Wwft) as well as Dutch penal law 138c. We have attached a separate legal opinion of this fact (that contains an Annex with English translation) that confirms this.

We understand that the Dutch detailed penal law and anti-money laundering law (which both prohibit the transaction processing of TMNL) may be complex. Yet, the topic is of high public interest and Journalist Platform Follow the Money also described how the personal data infringements occur for quite some years now without proper oversight. You can read this in the article: https://www.ftm.nl/artikelen/transactiemonitoring-banken-illegaal and you can also read our own web article which summarizes the case: https://hrif.eu/en/2024/04/tmnlstopuk/

We point out that footnote 10 of the attached legal opinion clarifies that the violation of the Dutch Penal Code does not require the intent to be specifically aimed at the unlawfulness. The question of whether the participating banks, TMNL or AWS itself are aware of the unlawfulness of these operations is not relevant. This means that, should Amazon continue processing for TMNL, it will be supporting and facilitating a Dutch criminal activity. We therefore kindly suggest and request AWS to stop their assistance to this criminal activity considering the harm done to both European and US persons involved and the inherent violation of GDPR article 6 which requires a lawful basis for processing of personal data.

We do understand of course that the Dutch legal specifics in this case are very nitty gritty and just as we don't know each detailed US law (like the recently time-extension of FISA section 702 which should protect US persons from being subject to monitoring), we do not expect AWS to understand the full details of the Dutch legal framework. For that reasons we will elaborate some further compliance details below that help you validate our viewpoint and decide to take swift action.

Outline of relevant legal articles
All banks in the Netherlands are fully aware that they may not outsource transaction monitoring under article 10 of the AML-Law. Since December 2020, the clarification of the Dutch Central Bank on the full prohibition on outsourcing of transaction monitoring is clearly stipulated on page 52 of the Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act (December 2020 version), which law has not changed since then:

> *Monitoring of the business relationship may, however, only be carried out by the institution itself.67*

Footnote 67 further explains:

> *This is because Section 3(2)(d) of the Wwft is not referred to in Section 10(1) of the Wwft. In the case of institutions governed by the Wft, and where the executing party is a member of the same group, such constant monitoring may be carried out by this party within the group.*

While Dutch banks have, behind the screens, tried to convince the Ministry of Finance that their transaction monitoring processing at TMNL was minimal in scope and not unlawful, they have overlooked the Dutch Penal Code and both the AML-supervisor DNB and the GDPR-supervisor Autoriteit Persoonsgegevens now have pending enforcement discussions on this matter.

Do also note that the legal opinion already stipulates the unlawfulness on the basis of the illegal outsourcing, but a number of other legal rules (processing sensitive personal data) also apply, leading to inherent unlawful processing of personal data by TMNL. In addition, with its letter of July 14, 2023, the Dutch Data Protection has made it clear that even should an explicit legal provision be in place, the outsourced transaction monitoring processing would still remain unlawful under EU rules (Kenmerk z2023-02465). TMNL holds a data pool and mass surveillance mechanism -encompassing the whole Dutch society- which breaches fundamental human rights.

Please stop immediately and fully delete all data, programs and algorithms
As the illegal data processing now pertains to more than 10 billion data subjects we do expect AWS to have ended their involvement with TMNL fully by the end of this month. **We hold AWS accountable and liable for not having performed proper due diligence on the operations of TMNL and for not having double checked the legislative developments in the Netherlands** on this topic (which were hard to miss due to the controversies in Parliament on this matter).

In the same vein, we think that the distribution and processing of AWS for Dutch banks: ING, Rabobank, ABN AMRO, Volksbank and Triodosbank, should audited and reviewed in order to ensure that all those banks (if they are AWS customer, such as Volksbank) comply with article 10 Wwft and do not infringe on Penal Law Code 138c. This could be done simply by those banks by immediately stopping their operations to send and receive transaction data from and to TMNL.

For your information: we have repeatedly requested further information from TMNL on their legal status and operations and they have refused to provide it. Similarly we have taken up actions towards banks, TMNL, the Dutch Bankers Association and used media to outline our viewpoint as well as litigation (which is now pending with a law suit planned in September 2024 at the Court of Rotterdam). While behind the screens, TMNL at the end of 2023 was pleading with the Dutch central bank, to not be regarded as 'outsourcing', TMNL refuses to take its responsibility towards customers and involved entities such as HRIF.EU (our data and that of our donors) by shutting down their unlawful operations.

Regardless of these 'local' Dutch discussions, it remains an independent AWS business decision to choose to comply with Dutch Penal Law as well as with the Anti-Money Laundering Law and the European GDPR. In this respect we have high regard of the Amazon legal professionality and its business capability to understand the relevance of lawfulness of data processing in an era which will soon also include big data processing under the rules of the European AI Act.

Our expectations, position and copy to Dutch Data Protection Authority

We trust you will understand our request and its ramifications and that AWS will do the right thing and respect the European rules. It would be hard to explain to the government business customers in other EU countries that AWS was involved in unlawful processing of the data of the whole Dutch society. Rather AWS would want to signal to those customers that it takes the fundamental rights of EU citizens serious (which we see as the added value and core capability of AWS here in Europe).

We therefore look forward to your urgent confirmation that all data and algorithms of TMNL have been deleted from primary and backup sites. This would in our view imply that the operations of AWS for TMNL no longer qualify as supporting the transgression of Dutch Penal Code, GDPR article 6 and AML-law article 10. And we will thus also explain this matter to the public and will applaud the immediate standstill by AWS. We are also open to writing a joint press statement underlining the professionality and capability of AWS to identify and correct unintended infringements of privacy.

Meanwhile, in a legal sense, we must also reserve all rights on behalf of all the data subjects, whose privacy has been infringed so massively. Those include our donors and the almost 15.000 Dutch citizens who signed up to our petition against massive unlaw payments monitoring in the Netherlands.

To ensure prompt action by AWS we will send a copy of this letter to [redacted] of the Dutch Data Protection Authority.

Yours sincerely,
Human Rights in Finance.EU

Simon Lelieveldt
Chairman

Copy:
- [redacted], Autoriteit Persoonsgegevens

Annex:
- Legal Opinion Attorney Dr. K.H. Zeegers, June 20, 2024 (p 4-10 with English annex

Annex: Translation: Legal Opinion regarding the Potential Criminality of Banks Data Pooling and Outsourcing operations with Transaction Monitoring Netherlands

Disclaimer: this is an (unofficial) translation of the preceding Dutch text; in case of any discrepancy, the original Dutch text prevails.

Dear Sir/Madam,

At the request of the Human Rights in Finance Foundation (hereinafter referred to as "**HRIF**"), this legal opinion examines whether the sharing of bank data by ABN AMRO, ING, Rabobank, Triodos Bank, and Volksbank with the entity they established, Transaction Monitoring Netherlands B.V. (hereinafter referred to as "**TMNL**"), can be qualified as a criminal offense under Article 138c of the Dutch Penal Code (hereinafter referred to as "**DPC**").

1. Background

TMNL was founded on July 10, 2020, by five Dutch banks: ABN AMRO, ING, Rabobank, Triodos Bank, and Volksbank. The intended purpose of establishing TMNL was to join the transaction monitoring of these banks with respect to their business clients. The added value of TMNL was thought to lie in the fact that individual banks can only identify potentially unusual transaction that flow through accounts at their own bank, while criminals often spread money flows across multiple banks. By pooling information from the participating banks and centralizing the monitoring activities at TMNL, better insight into potentially unusual transaction flows is thought to be achieved.[1] This is all done within the framework of banks' obligations regarding transaction monitoring under the Anti-Money Laundering and Anti-Terrorist Financing Act (hereinafter referred to as the "**AML/CTF Act**").

To achieve this objective, the five banks involved share all transaction data regarding their business clients with TMNL. This includes business transactions of small and medium-sized enterprises with a turnover of up to 250 million euros, including transactions of sole proprietorships. Additionally, transactions between individuals and the mentioned businesses are included.[2] TMNL analyses the data received and reports back to each individual participating bank based on the combined data. As a result, the banks effectively grant both TMNL and each other access to their transaction data. Subsequently, TMNL sends alerts back to the individual banks. Each individual bank then links these alerts to the exact customer involved, and should further investigate the alert, which, in turn, may lead to reports of unusual transactions to the Financial Intelligence Unit Netherlands (which is a part of the Dutch Public Prosecutor's Office).

2. Analysis of Relevant Legal Provisions

The obligation of banks to conduct transaction monitoring is established in the AML/CTF Act. Article 3 of the AML/CTF Act stipulates that banks (as "institutions" within the meaning of Article 1 of the AML/CTF Act) are required to conduct 'client investigations'. Subparagraphs a through f of the second paragraph of Article 3 of the AML/CTF Act further elaborate on the components of such client investigations. The obligation of banks to conduct transaction monitoring follows from Article 3, paragraph 2, subparagraph d of the AML/CTF Act, which defines this obligation as follows: *"to exercise ongoing monitoring of the business relationship and the transactions carried out during the duration of this relationship, in order to ensure that they correspond with the knowledge the institution has of the client and their risk profile, including, where necessary, an investigation into the source of the funds used in the business relationship or the transaction."*

[1] Webpagina TMNL, "over ons" < https://tmnl.nl/over-tmnl/tmnl-in-het-kort/ > (geraadpleegd op 24 mei 2024).
[2] Bron: toelichting HRIF.EU op grond van informatie uit: Kamerstukken II 2022/23, 36228, nr. 3 (MvT), p. 25.

Article 10, paragraph 1 of the AML/CTF Act then creates the possibility for banks to outsource the client investigation and have it conducted by a third party (in the context of an outsourcing or agency agreement). However, this outsourcing authority exists solely with respect to the components of the client investigation described in Article 3, paragraph 2, subparagraphs a, b, c, e, and f of the AML/CTF Act. As previously stated, the obligation to conduct transaction monitoring is described in subparagraph d of Article 3, paragraph 2 of the AML/CTF Act, and this subparagraph is explicitly excluded from the outsourcing authority.

Therefore, the AML/CTF Act does not permit banks to outsource the performance of their obligation to conduct transaction monitoring to third parties.

Article 138c of the Dutch Penal Code (DPC) criminalizes: *"the intentional and unlawful acquisition or transmission of non-public data stored by means of an automated process for oneself or another"*. This provision was introduced by the "Computer Crime Act III" and came into effect in 2019,[3] aiming to enhance the criminal protection of data stored by automated means.[4]

This provision is directed at those who have lawful access to non-public data stored digitally and unlawfully acquire or transmit this data to another party. The term 'transmission' was added to the provision in 2021.[5] The legislative history indicates that non-public data refers to all data that the public does not have access to.[6] The provision criminalizes only the *unlawful* acquisition or transmission of such data. There is no such unlawfulness if the data is acquired or transmitted with the consent of the rightful owner of the data, or if there is a legal basis for the acquisition/transmission of the data.[7] A third potential exception to the criminality of unlawfully acquiring or transmitting such data, mentioned in the legislative history, is when it doing so falls within the scope of the right to freedom of expression or press freedom, as protected by Article 10 of the European Convention on Human Rights (hereafter: "**ECHR**"); this exception is intended to protect whistleblowers and journalists. Specifically, this means that the transmission of bank data to (or its acquisition by) whistleblowers or journalists, should not qualify as a criminal offense under Article 138c DPC, because that would violate Article 10 ECHR.

3. Conclusion

With the establishment of TMNL, a private limited company and independent (legal) entity, the five participating banks have outsourced the execution of transaction monitoring concerning their business clients to a third party. TMNL analyses the transaction data received from the participating banks and reports its findings back to each of these banks. To enable TMNL to carry out its intended tasks, the five participating banks continuously share all transaction data of all their business clients with TMNL. Because TMNL shares its analysis of the combined transaction data with the participating banks, these banks effectively share their transaction data with each other through TMNL. Furthermore, TMNL's reporting back to the individual banks qualifies as a violation of Article 138c DPC by TMNL itself.

Such transaction data clearly qualifies as *"non-public data stored by means of an automated process"* within the meaning of Article 138c DPC. Additionally, the sharing of these data evidently qualifies as *"transmission"* within the meaning of the same provision. The key question is whether the transmission of such data can also be considered unlawful.

[3] Wet van 27 juni 2018, Stb. 2018, 322, inwerkingtreding 1 maart 2019.
[4] NLR aant. 1 ad art. 138c WvSr.
[5] NLR aant. 2 ad art. 138c WvSr.
[6] Kamerstukken II 2015/16, 34372, nr. 3 (MvT), p. 66.
[7] Kamerstukken II 2015/16, 34372, nr. 3 (MvT), p. 66.

As noted, there is currently no explicit legal basis for the sharing of information by banks with TMNL (and vice versa). This also follows from the legislative history of the upcoming Anti-Money Laundering Action Plan Act.[8] This law aims to introduce a legal basis for joint transaction monitoring for banks.[9] It logically follows from this that the legislature recognizes that such a legal basis does not currently exist. Additionally, this law aimed to introduce a legal basis for outsourcing transaction monitoring by banks to third parties. The Explanatory Memorandum of this law indicates that this is currently not possible – it is explicitly considered that with the introduction of such a basis, *"a legal obstacle [is] removed."* This implies that this obstacle still exists at present.

In conclusion: There is no legal basis or authority for banks to transmit transaction data to TMNL – the establishment of TMNL is an independent initiative of the participating banks. The transmission of this data therefore appears to qualify as unlawful. Furthermore, as noted earlier, the AML/CTF Act prohibits financial institutions from outsourcing their obligation to conduct transaction monitoring to third parties. Specifically, the authority to outsource components of client investigation to third parties explicitly excludes transaction monitoring.

The transmission of banking transaction data from business clients by ABN AMRO, ING, Rabobank, Triodos Bank, and Volksbank to TMNL (and, via TMNL, to the other participating banks) thus fulfils all elements of the offense described in Article 138c of the Dutch Penal Code and can therefore be considered a criminal offense.[10] Additionally, the feedback provided by TMNL to individual banks also qualifies as such, as it involves transmitting processed information that was initially unlawfully obtained.

Thank you in advance for your time and attention.

Signed

K.J. (Krit) Zeegers (Ph.D. LL.M.), Attorney at Prakken d'Oliveira Human Rights Lawyers in Amsterdam

[8] This proposed law is still pending before the second chamber of the Dutch parliament: <https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoors tel%3A36228>

[9] Kamerstukken II 2022/23, 36228, nr. 3 (MvT), p. 11.

[10] It should be noted that Article 138c DPC does not require the intent to be specifically aimed at the unlawfulness, so the question of whether the participating banks are aware of the unlawfulness of their practice is not relevant. See Tekst & Commentaar aant. 8 ad art. 138c Sr: *"Intent is included as an element in the offense description. It encompasses, according to the currently widely accepted views, all degrees of intent, including conditional intent. It is directed at all elements of the crime, except unlawfulness." (Translation KZ).*