

VIA MAIL AND E-MAIL TO: [abuse@amazonaws.com](mailto: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

[REDACTED] and 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.<sup>67</sup>*

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 professionalism 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 professionalism 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], director 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

LINNAEUSSTRAAT 2 -A, 1092 CK AMSTERDAM  
TELEFOON +31(0)20-3446200 | FAX +31(0)20-3446201  
E-MAIL: [info@prakkendoliveira.nl](mailto:info@prakkendoliveira.nl) | [www.prakkendoliveira.nl](http://www.prakkendoliveira.nl)

MARQ WIJNGAARDEN  
FLIP SCHÜLLER  
PROF. LIESBETH ZEGVELD  
MARIEKE VAN EIK  
WIL EIKELBOOM  
DR. CHANNA SAMKALDEN  
TAMARA BURUMA  
BONDINE KLOOSTRA  
MICHIEL PESTMAN  
BRECHTJE VOSSENBERG  
EVA BEZEM  
EMIEL JURJENS  
DR. LISA-MARIE KOMP  
BARBARA VAN STRAATEN  
TOM DE BOER  
DR. KRIT ZEEGERS  
FREDERIEKE DÖLLE  
ELLES TEN VERGERT  
ISA VAN KRIMPEN  
DORA BROUWER  
THOMAS VAN DER SOMMEN  
LARAB MOHAMMAD  
SHRUTI TOELSIE

*ADVISEURS*

PROF. HANS ULRICH JESSURUN D'OLIVEIRA  
PROF. TIES PRAKKEN

Amsterdam, 20 juni 2024

Onze ref. D20231270 [REDACTED]

E-mail: [REDACTED]

**Betreft: Juridische Opinie m.b.t. mogelijke strafbaarheid van het delen van transactiegegevens door banken met Transactiemonitoring Nederland**

Geachte,

Op verzoek van Stichting Human Rights in Finance (hierna: "HRIF") wordt in deze juridische opinie onderzocht of het delen van bankgegevens door ABN AMRO, ING, de Rabobank, Triodos Bank en de Volksbank met de door hen opgerichte entiteit Transactie Monitoring Nederland B.V. (hierna: "TMNL"), kan worden gekwalificeerd als strafbaar feit op grond van artikel 138c van het Wetboek van Strafrecht (hierna: "WvSr").

Hieronder wordt eerst een toelichting gegeven op de oprichting en werkwijze van TMNL. Daarop volgt een analyse van relevante wetsbepalingen, mede aan de hand van de wetsgeschiedenis en literatuur. Tot slot wordt de hiervoor geformuleerde vraag die de aanleiding vormt van deze analyse, beantwoord. Een korte Engelse vertaling is opgenomen in de bijlage.

## 1. Oprichting en werkwijze TMNL

TMNL is op 10 juli 2020 opgericht door vijf Nederlandse banken: ABN AMRO, ING, de Rabobank, Triodos Bank en de Volksbank. Het beoogde doel van de oprichting van TMNL, was het samenbrengen van de transactiemonitoring van deze banken wat betreft hun zakelijke klanten. De toegevoegde waarde van TMNL zou erin liggen, dat individuele banken enkel zicht hebben op mogelijk ongebruikelijke transactiestromen via rekeningen bij de eigen bank, terwijl criminelen dergelijke geldstromen juist vaak spreiden over verschillende banken. Door de informatie vanuit deelnemende banken te bundelen en de monitoringsactiviteiten bij TMNL onder te brengen, zou beter zicht ontstaan

op mogelijke ongebruikelijke transactiestromen.<sup>1</sup> Dit alles in het kader van de verplichtingen van banken op het gebied van transactiemonitoring op grond van de Wet ter voorkoming van Witwassen en Terrorismefinanciering (hierna: “Wwft”).

Ter verwezenlijking van dit doel, delen de vijf betrokken banken alle transactiegegevens van hun zakelijke klanten met TMNL. Het betreft zakelijke transacties van het midden- en kleinbedrijf met een omzet tot 250 miljoen euro, waaronder ook begrepen transacties van eenmanszaken. Daarnaast zijn transacties tussen de particulieren en genoemde bedrijven opgenomen.<sup>2</sup> TMNL analyseert deze bankgegevens en rapporteert, op basis van de gecombineerde gegevens, terug aan iedere individuele deelnemende bank. Daarmee verlenen de banken zowel aan TMNL als aan elkaar inzage in deze transactiegegevens. Vervolgens stuurt TMNL alerts terug aan individuele banken. Deze worden door de individuele banken worden gekoppeld aan de precieze klant, worden nader onderzocht en kunnen bij vermoeden van een ongebruikelijke transactie leiden tot een melding ongebruikelijke transacties bij de Financial Intelligence Unit Nederland.

## 2. Analyse relevante wetsbepalingen

De verplichting van banken tot het verrichten van transactiemonitoring is vastgelegd in de Wwft. Artikel 3 Wwft bepaalt dat banken (als “instelling” in de zin van artikel 1 Wwft) verplicht zijn tot het verrichten van ‘cliëntenonderzoek’. In subparagraaf a t/m f van het tweede lid van artikel 3 Wwft wordt nader uitgewerkt waaruit dergelijk cliëntenonderzoek dient te bestaan. De verplichting van banken tot het verrichten van transactiemonitoring volgt uit artikel 3 lid 2 sub d. Wwft, dat deze verplichting als volgt definieert: *“een voortdurende controle op de zakelijke relatie en de tijdens de duur van deze relatie verrichte transacties uit te oefenen, teneinde te verzekeren dat deze overeenkomen met de kennis die de instelling heeft van de cliënt en diens risicoprofiel, met zo nodig een onderzoek naar de bron van de middelen die bij de zakelijke relatie of de transactie gebruikt worden”*.

Artikel 10 lid 1 Wwft schept vervolgens een mogelijkheid voor banken om het cliëntenonderzoek uit te besteden en te laten verrichten door een derde (in het kader van een uitbestedings- of agentuurovereenkomst). Deze uitbestedingsbevoegdheid bestaat echter uitsluitend ten aanzien van de onderdelen van het cliëntenonderzoek omschreven in artikel 3 lid 2 subparagrafen a., b., c., e., en f. Wwft. Zoals hiervoor gezegd wordt de verplichting tot transactiemonitoring omschreven in sub d. van artikel 3 lid 2 Wwft, en deze subparagraaf wordt expliciet uitgezonderd van de bevoegdheid tot uitbesteding.

De Wwft staat het banken dus niet toe om de uitvoering van hun verplichting tot transactiemonitoring uit te besteden en te laten verrichten door derden.

Artikel 138c WvSr stelt strafbaar: het *“opzettelijk en wederrechtelijk, voor zichzelf of voor een ander overnemen of doorgeven van niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk”*. Deze strafbepaling is ingevoerd door de Wet Computercriminaliteit III en in

<sup>1</sup> Webpagina TMNL, “over ons” < <https://tmnl.nl/over-tmnl/tmnl-in-het-kort/> > (geraadpleegd op 24 mei 2024).

<sup>2</sup> Bron: toelichting HRIF.EU op grond van informatie uit: Kamerstukken II 2022/23, 36228, nr. 3 (MvT), p. 25.

2019 in werking getreden,<sup>3</sup> en heeft tot doel om de strafrechtelijke bescherming van gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, te verbeteren.<sup>4</sup>

Deze strafbepaling is gericht tot degene die zelf rechtmatig toegang heeft tot niet-openbare gegevens die digitaal zijn opgeslagen, en deze gegevens – onrechtmatig – overneemt of doorgeeft aan een ander. Het ‘doorgeven’ is in 2021 toegevoegd aan de strafbepaling.<sup>5</sup> Uit de wetsgeschiedenis blijkt dat met niet-openbare gegevens wordt bedoeld, alle gegevens waartoe het publiek geen toegang heeft.<sup>6</sup> De bepaling stelt alleen strafbaar het *wederrechtelijk* overnemen of doorgeven van dergelijke gegevens. Deze vereiste wederrechtelijkheid ontbreekt als de gegevens zijn overgenomen of doorgegeven met toestemming van de rechthebbende, of wanneer een wettelijke bevoegdheid daartoe bestaat.<sup>7</sup> Een derde uitzondering op de strafbaarheid van het overnemen of doorgeven van dergelijke gegevens die wordt genoemd in de Memorie van Toelichting, is wanneer dit gebeurt ter uitoefening van het recht op vrijheid van meningsuiting en de persvrijheid, beschermd door artikel 10 van het Europees Verdrag ter bescherming van de Rechten van de Mens (hierna: “EVRM”); dit ter bescherming van klokkenluiders en journalisten. Concreet betekent dit dat het overnemen van bankgegevens door klokkenluiders, of het doorgeven daarvan aan journalisten, niet kwalificeert als strafbaar feit in de zin van artikel 138c WvSr, omdat dit in strijd zou zijn met artikel 10 EVRM.

### 3. Conclusie

Met de oprichting van TMNL, een besloten vennootschap en zelfstandige (juridische) entiteit, hebben de vijf deelnemende banken het uitvoeren van transactiemonitoring met betrekking tot hun zakelijke kanten uitbesteed aan een derde. TMNL analyseert de transactiegegevens die van de deelnemende banken zijn ontvangen en rapporteert zijn bevindingen terug aan ieder van deze banken. Om TMNL in staat te stellen zijn beoogde taken uit te voeren, delen de vijf deelnemende banken, op doorlopende basis, alle transactiegegevens van al hun zakelijke klanten met TMNL. Doordat TMNL zijn analyse van deze gecombineerde transactiegegevens deelt met de deelnemende banken, delen deze banken hun transactiegegevens effectief ook met elkaar, via TMNL. Voort deelt TMNL de uitkomsten met individuele banken, met als gevolg dat ook de terugmelding van TMNL kwalificeert als overtreding door TMNL van artikel 138c WvSr.

Dergelijke transactiegegevens kwalificeren evident als *“niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk”* in de zin van artikel 138c WvSr. Het delen van deze gegevens kwalificeert voorts evident als *“doorgeven”* in de zin van diezelfde bepaling. De kernvraag is of het doorgeven van deze gegevens ook als wederrechtelijk – onrechtmatig – kan worden aangemerkt.

Zoals opgemerkt bestaat op dit moment geen expliciete wettelijke grond voor informatiedeling door banken met TMNL (en vice versa). Dit volgt uit de wetsgeschiedenis van de aankomende Wet plan van

---

<sup>3</sup> Wet van 27 juni 2018, Stb. 2018, 322, inwerkingtreding 1 maart 2019.

<sup>4</sup> NLR aant. 1 ad art. 138c WvSr.

<sup>5</sup> NLR aant. 2 ad art. 138c WvSr.

<sup>6</sup> Kamerstukken II 2015/16, 34372, nr. 3 (MvT), p. 66.

<sup>7</sup> Kamerstukken II 2015/16, 34372, nr. 3 (MvT), p. 66.

aanpak Witwassen.<sup>8</sup> Deze wet beoogt een wettelijke grondslag te introduceren voor gezamenlijke transactiemonitoring voor banken.<sup>9</sup> Hieruit volgt logischerwijs dat de wetgever erkent dat zo'n wettelijke grondslag thans nog niet bestaat. Daarnaast beoogt deze wet een wettelijke grondslag te introduceren voor het *uitbesteden* van transactiemonitoring door banken aan derden. Uit de Memorie van Toelichting van deze wet blijkt dan ook dat dit thans nog niet mogelijk is – expliciet wordt overwogen dat met de introductie van zo'n grondslag “*een wettelijke belemmering [wordt] weggenomen.*”<sup>10</sup> Hieruit kan worden afgeleid dat deze belemmering op dit moment nog geldt.

Concluderend: Er is geen wettelijke grond of bevoegdheid voor het doorgeven van de transactie gegevens door banken aan TMNL – de oprichting van TMNL is een zelfstandig initiatief van de deelnemende banken. Het doorgeven van deze gegevens lijkt dan ook te kwalificeren als wederrechtelijk. Te meer nu, zoals hiervoor is opgemerkt, de Wwft financiële instellingen verbiedt om hun verplichting tot transactiemonitoring uit te besteden aan derden. Althans, de bevoegdheid om onderdelen van het cliëntenonderzoek wél uit te besteden aan derden, sluit transactiemonitoring expliciet uit.

Het doorgeven van bancaire transactiegegevens van zakelijke klanten door ABN AMRO, ING, de Rabobank, Triodos Bank en De Volksbank aan TMNL (en, via TMNL, aan de andere deelnemende banken) vervult daarmee alle bestanddelen van de delictsomschrijving uit artikel 138c Sr en kan daarmee worden aangemerkt als strafbaar feit.<sup>11</sup> Ook de terugmeldingen van TMNL aan individuele banken kwalificeert als zodanig nu zij voor de banken (de ander) een bewerking van de eerder onrechtmatige informatie doorgeeft.

Bij voorbaat dank voor uw tijd en aandacht.

Met vriendelijke groet,



mr. dr. K.J. (Krit) Zeegers, advocaat bij Prakken d'Oliveira Human Rights Lawyers te Amsterdam

---

<sup>8</sup> Dit wetsvoorstel is nog aanhangig bij de Tweede Kamer, zie <<https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A36228>>

<sup>9</sup> Kamerstukken II 2022/23, 36228, nr. 3 (MvT), p. 11.

<sup>10</sup> Kamerstukken II 2022/23, 36228, nr. 3 (MvT), p. 11.

<sup>11</sup> Ten overvloede merk ik op dat artikel 138c WvSr niet vereist dat sprake is van opzet op de wederrechtelijkheid, zodat de vraag of de deelnemende banken zich bewust zijn van de wederrechtelijkheid van deze werkwijze, niet relevant is. Zie Tekst en Commentaar aant. 8 ad art. 138c WvSr: “*Het opzet is als bestanddeel in de delictsomschrijving opgenomen. Het omvat, naar de thans vrij algemeen aanvaarde opvattingen alle gradaties van opzet, inclusief het voorwaardelijk opzet. Het is op alle bestanddelen van de delictsomschrijving gericht, behoudens de wederrechtelijkheid.*”

**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.<sup>1</sup> 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.<sup>2</sup> 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."*

---

<sup>1</sup> Webpagina TMNL, “over ons” < <https://tmnl.nl/over-tmnl/tmnl-in-het-kort/> > (geraadpleegd op 24 mei 2024).

<sup>2</sup> 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,<sup>3</sup> aiming to enhance the criminal protection of data stored by automated means.<sup>4</sup>

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.<sup>5</sup> The legislative history indicates that non-public data refers to all data that the public does not have access to.<sup>6</sup> 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.<sup>7</sup> 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.

---

<sup>3</sup> Wet van 27 juni 2018, Stb. 2018, 322, inwerkingtreding 1 maart 2019.

<sup>4</sup> NLR aant. 1 ad art. 138c WvSr.

<sup>5</sup> NLR aant. 2 ad art. 138c WvSr.

<sup>6</sup> Kamerstukken II 2015/16, 34372, nr. 3 (MvT), p. 66.

<sup>7</sup> 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.<sup>8</sup> This law aims to introduce a legal basis for joint transaction monitoring for banks.<sup>9</sup> 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.<sup>10</sup> 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

---

<sup>8</sup> This proposed law is still pending before the second chamber of the Dutch parliament:

<[https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorstel&qry=wetsvoors\\_tel%3A36228](https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorstel&qry=wetsvoors_tel%3A36228)>

<sup>9</sup> Kamerstukken II 2022/23, 36228, nr. 3 (MvT), p. 11.

<sup>10</sup> 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).