AMLC

NEWSLETTER DECEMBER 2021

Anti Money Laundering Centre

Dear colleague,

This is the last AMLC newsletter for 2021: **an extra big end-of-the-year edition!**

We look back on a year with once more, a lot of 'remote cooperation'. Luckily, we do find ever more ways to find each other. We recently found that the *on-site* of the FATF could actually take place in Corona times and we express our thanks to the excellent organizational team and we appreciate the flexibility of all those involved, which made it possible to go through with the event in Corona times. This newsletter sets out how the visit went and what the follow-up will be.

This newsletter also pays attention to TBML, crime scripting, a podcast on crowdfunding and an article on the concrete and verifiable statement of the suspect in step-by-step cases. Furthermore, this edition contains an in-depth article on cooperation between banks and investigation.

As you have come to expect from us, we close with case law. This time about a fine imposed on a trust office, the UBO register, the gatekeeper role of the civil-law notary and a terminated banking relationship with a telecom company.

In the event you have had experiences or you have come across constructions you wish to share, please send an email to AML.Centre_Postbus@belastingdienst.nl. If you have any colleagues who would like to get the newsletter, they can register via this email address. And to conclude, if you wish to be up-to-date, follow us on LinkedIn!

We hope you enjoy reading this newsletter,

The AMLC

ANTI MONEY LAUNDERING CENTRE

News

A specific and verifiable statement

AMLC colleagues Suzanne Visser and Ruut Regtering wrote a contribution for the most recent issue of the Magazine for Criminal law and Enforcement (*Tijdschrift voor Bijzonder Strafrecht & Handhaving*) which sets out a step-by-step plan in respect of money laundering. The article contains case law in relation to a specific and verifiable statement from a suspect where money laundering is suspected. In practice, it is a question that is often unclear, i.e., whether a statement is sufficiently specific and verifiable, whilst the answering of that question is essential to the continuing course and the possible outcome of a case. The authors give an outline in this article of the conclusions from case law and court rulings and they give recommendations to determine in practice, whether a statement must be verified or not. Click here for the full article.

A new prosecution directive in respect of money laundering

A new prosecution directive for money laundering was recently published. The Public Prosecutor now has points of reference for money laundering cases to formulate a demand. Incidentally, judges have no national reference points for imposing sentences in cases concerning money laundering. There are reference points for fraud cases but these are not specific to cases of money laundering. *mr. dr.* W.S. de Zanger recently argued in the Magazine for Criminal law and Enforcement (*Tijdschrift voor Bijzonder Strafrecht & Handhaving* or TBS&H) for further reflections of our 'own' judicial reference points for money laundering.

Cooperation of the AMLC with the Utrecht University

The AMLC focus on money laundering includes the use of trade flows, or Trade-Based Money Laundering. In this context, a good risk-based project is currently the subject of much work. Over the last few years, in a public and private context, a lot of knowledge about the trade sectors was acquired from what we came across in criminal investigations. Think of the car trade, the fruit and vegetables sector. We cooperated with financial institutions and we are mainly aware of Trade-Based Money Laundering or TBML indicators which have been generated using transaction data.

However, there are many more relevant sources, think of tax data, or data relating to the – illogical – flow of goods such as at Customs. On a daily basis, millions of goods are being traded in a country like the Netherlands and it is of importance to get more of a view of these sources. In the time to come, we are therefore going to invest into the identification of vulnerable points in the Dutch flows of trade. We are collaborating with Joras Ferwerda, research fellow of Utrecht University. This collaboration will provide us with a view on several issues. What sectors in the Netherlands are vulnerable to Trade-Based Money Laundering (TBML) and why? What are the signs Customs must look for on where the checking of export is concerned? What signs should be

the focus of the various sectors themselves? We were fortunate to be able to use the experiences of the HMRC (Her Majesty's Revenue & Customs) and the ABF (Australian Border Force). In addition to gaining more knowledge, this methodology generated new signs which can be the subject of further judicial investigations. For more information, please contact our TBML expert, Tamara Pollard: tw.pollard-maijer@belastingdienst.nl

New AMLC-podcast

The latest podcasts concentrate on the risks of crowdfunding by two staff members of the Financial Supervision Office (*Bureau Financieel Toezicht* or BFT). How can assets proceeding from crime be used by way of crowd funding to buy immovable property? What do civil-law notaries have to watch out for? These questions and many more are discussed. In addition, the 'Regulation (EU) on European providers of crowdfunding service providers for business' that recently came into force is also a topic on the basis of which certain crowd funding service providers are now obliged to have a licence. For more information on this topic, go to the website of AFM, which includes a helpful brochure.

FATF evaluation Netherlands

The Financial Action Task Force or FATF makes periodical evaluations of different countries. Such an evaluation starts on the basis of what is referred to as a *Mutual Evaluation*, in which a team of experts from a variety of countries is asked to make an evaluation of a country in accordance with a standard procedure. The implementation of recommended measures (*40 Recommendations*), effectiveness (*11 Immediate Outcomes*) of the country in combating money laundering, the financing of terrorism and proliferations form part of the points that are the subject of the evaluation.

A visit was made to the Netherlands in the period from 27 October to 18 November 2021 (*on-site*) as part of this process by '*financial, legal and law enforcement experts*' from Austria, Belgium, Brazil, Hong Kong, China, Japan and the Sultanate of Oman, with the support of members of the administrative office of FATF. The experts had already been provided with the necessary documents prior to the visit; more than 2000 pages of text and supporting information, 200 case descriptions and 54 descriptions of projects and collaborative arrangements, which meant that there was enough for substantive discussions with 138 representatives from public parties as well as representatives from 38 private parties. The event took place at a height of 146 metres on the 36th floor of the Ministry of Justice and Security and during the many meetings, numerous questions were fired to different persons attending. However, all those present were given the opportunity to show the effectiveness or to make those aware of the possible problems they came across. The circumstances were not ideal as a result of Covid but it was successful with certain adjustments everyone made and more than 100 self-tests. FATF expressly thanked the Netherlands and all those who made their contributions; the flexibility, the thorough preparation as well as all the documents as provided were much appreciated. So how to go on? Prior to *on-site*, the team of experts had already given a first draft response to the *40 recommendations* which particularly monitor the legal-technical basis in the Netherlands, and the presented document will be supplemented to form a total report which also considers the 11 components in the context of the effectiveness of the way the Netherlands tackles these issues. The first draft version is expected to be offered to the Dutch representation at the beginning of the first quarter 2022. Eventually, in June 2022, the report is adopted

during a plenary session of FATF as well as being released for publication. We have to wait for the final evaluation and the recommendations for the Netherlands, but we will keep you informed! If you wish to have more information about the process of mutual evaluations, click here or listen to the various AMLC podcasts on this topic via your favourite podcast app.

Crime scripting
Earlier we reported on fincancial crime scripting (read here - login required). Those who want to know more about crime scripting can read this scientific article by Thom Snaphaan, criminologist at the Public Prosecution Service (Follow the Money). Next year, in collaboration with a college of higher education, we will explore how crime scripting can be helpful in the context of combating money laundering.

Banks have a wealth of information

Gitty Kanters, FIOD Eindhoven

Introduction
Recently the Fiscal Intelligence and Investigation Service (*Fiscale Inlichtingen- en Opsporingsdienst* or FIOD) conducted a criminal investigation further to the ING Bank having reported an incident to the Police. This report proved to be the beginning of finding a goldmine of information. The result was that seven suspects were arrested who presumably formed part of a criminal organization involved in substantial fraud as well as the use of many 'money mules' who were being used to launder the money obtained.

This article aims to once more inform the banks of the interest in their role of detecting financial crime. In addition, we wish that investigating officers or financial investigating officers draw on the use of technical/identifying data which are available to banks and which proved to be of crucial importance in the investigation concerned.[1]

What was it that made ING's information so valuable to the FIOD investigation?
The reason for ING reporting the incident was a detection signal from an account which had **conspicuous transactions** (read: a-typical transactions for the account holder, i.e., a substantial credit from abroad followed by an immediate withdrawal in cash). Subsequently, ING conducted investigations into the various devices that had been logged in on the personal *MijnING* account (electronic banking) of the account holder concerned (ING assigns a **unique DeviceID** to devices logging in. They subsequently provided an overview of the DeviceID's that had logged into the accounts of several accountholders. It showed the same conduct in relation to conspicuous transactions as was shown in the accounts of other accountholders. This information was clearly set out in the report of the incident. In addition, it contained the information that was known as to which **DeviceTag** (the name a user can give to a device) belonged to a DeviceID. This information proved of prime importance when it came to identifying the first suspect. At a later point, a cookie was found on the telephone of this suspect showing a DeviceID which was used for

[1] As an investigating officer, consider what information can be of additional value to the investigation. In addition to the proportionality test and the subsidiarity test carried out by the Public Prosecutor, such considerations prevent banks from getting too much unnecessary work.

several accountholders referred to in the report of the incident. The report of the incident and the appendices also contained the **IP addresses** associated with the login dates on the various *MijnING* accounts. These IP addresses could be linked to residential addresses after which they were compared to IP addresses which the suspects used at other moments in time. The report also contained **camera images** of the cash withdrawals as secured by the bank and these were added to the report of the incident. During the course of the investigations, it was possible to recognize the suspects, not being account holders.

Conclusion
In summary, it shows that in respect of this specific investigation, the bank included very valuable information in its report of the incident. The 'preparatory activities' by the bank proved of crucial importance to tracking down the presumably criminal organization. The accounts used by the purported criminal organization were presumably accounts from 'money mules'. Equally, these 'money mules' themselves, by making their accounts available have possibly committed a criminal offence. The file of the criminal case is currently at the Public Prosecutor's Service.
It is not known when the case comes to court.

Case law

District Court Rotterdam, 3 November 2021, A fine imposed on a trust office: ECLI:NL:RBROT:2021:10943
DNB imposed an administrative fine of € 100,000 on a trust office and informed this office that the decision will be published. The trust office did not agree and applied to the court by way of preliminary relief proceedings to suspend said decision until the court ruled as to whether the decision to impose a fine was lawful. The fine was imposed as the trust office failed to notify the FIU of the unusual transaction in good time, i.e. within 14 days. The transaction concerned consultancy fees charged by a party, whose registered office was in Panama, to another party, which concerned oil trade in or via Russia and Kazakhstan, involving Politically Exposed Persons (PEP's). The invoices sent deviated considerably from the consultancy agreement which served as the basis for the payments. The consultancy agreement stipulated that the one business paid the other business a fixed fee of USD 200,000 every month whilst the invoices covered a time span of 6 months and the invoices did not specify the activities that were carried out. Moreover, different amounts were charged than those agreed upon. There was furthermore an invoice for a bonus whilst it did not follow from the consultancy agreement. Due to the fact that it was not clear what the invoices as sent related to, in addition to deviations from the agreements on several points, the court held that the trust office was unable to establish that the invoices were actually linked to the activities carried out under the consultancy agreement. A trust office can be expected to meet high standards to prevent money laundering and every unusual transaction must be notified. As the trust office did not comply in good time, the FIU was not able to conduct an immediate investigation to inform the relevant institutions in respect of an unusual transaction. In addition, the

decision concerned is allowed to be published as publication is not disproportionate in this case. Possible damage to their reputation does not suffice to that end.

The division for notarial matters Amsterdam, 2 September 2021 (publication 1 November 2021), The gatekeeper role of the civil-law notary: ECLI:NL:TNORAMS:2021:22

In this case, a former civil-law notary was suspended for 6 months on account of insufficiently complying with the gatekeeper role in 2017 and 2018. The civil-law notary should have been alert for fraud indications. In this case, there were a number of files which involved the incorporation of private limited companies, whose incorporators did not have the Dutch nationality and they were not resident in the Netherlands. The files were furthermore received via an intermediary and there was no documentary evidence of correspondence with the incorporators and the address of the company was located in a multi-business building. Furthermore, in one of the files it turned out that a founding member of the private limited company lived at an address where homeless people can report for help. The civil-law notary did not signal the presence of a postal address, whereas she should have investigated this further. Indeed, these circumstances may indicate a money mule. There were also some doubts as to whether the activities of some of the companies – such as export and import – were able to be carried out from a multi-business building. The civil-law notary did not detect that it was a postal address, whilst he should have concluded that further searches had to be conducted. In addition, the civil-law notary did not keep to the obligations pursuant to the Money laundering and Terrorist Financing (Prevention) Act; it became evident from a proof of identity missing in three files and the civil-law notary failed to carry out more stringent searches. The latter was necessary as it was a matter of identification at a distance and because it was a matter of an increased risk of money laundering due to the nature of the transaction. Moreover, the civil-law notary failed to notify the unusual transactions to the Financial Intelligence Unit (FIU). The defence put forward by the civil-law notary that the current Money laundering and Terrorist Financing (Prevention) Act, which contains more stringent measures for client screening and the obligation to the investigate transactions without an obvious economic objective, did not apply at the time of executing the deed (January 2017 up to and including March 2018), but this defence did not hold. At the time, there already were manuals and notes available in which the open standard of – stringent – client screening had already been outlined by the Royal Dutch Association of Civil-law Notaries together with the Financial Supervision Office (BFT).

All businesses and legal entities in the Netherlands, as well as foreign companies with a branch in the Netherlands, must be entered in the Trade Register. A visiting address in the Trade Register is an obligation. The civil-law notary could have conducted more searches in this case into the address of the multi-business building. Seeing that it does not make sense that wholesale trade, retail trade, import and export take place from a multi-business building, in view of the limited storage facilities in such buildings.

District Court Amsterdam, 20 October 2021, The risk of money laundering in respect of a telecommunications business: ECLI:NL:RBAMS:2021:5997

This case concerns the question whether the ABN AMRO Bank was allowed to terminate the relationship with a telecommunications business on account of the risk of money laundering. The banking relationship was terminated as the company conducted business with clients the bank had under suspicion as a result of the fact that there were questions about a number of transactions. It was a matter of very substantial transactions – approximately amounting to 2 million Euros - that after coming into account were almost immediately transferred to foreign payment accounts. Approximately 25% of the turnover – approximately 2 million Euros – was being transferred to an entity in a high-risk country (United Arab Emirates) without any obvious link to the telecommunications provider. In addition, many

of the clients of the telecommunications provider transferred substantial amounts in a short time, but in the meantime, they no longer exist, whilst only recently having been incorporated. The clients frequently concerned ABN AMRO clients with whom the bank in the meantime terminated the banking relationship as a result of an actual risk of money laundering. Despite the fact that it might well be possible that the company may be a rarity among the telecommunications providers, the court in preliminary relief proceedings held that the Bank was allowed to terminate the relationship on the basis of the risk profile.

The Court of Appeal agrees with the decision of the court in preliminary relief proceedings in the case of the Ultimate Beneficial Owners (UBO) register (ECLI:NL:GHDHA:2021:2176)

On 16 November 2021, the Court of Appeal in The Hague decided that the Dutch legislation in respect of the Ultimate Beneficial Owners register does not have to be suspended. This ruling means that the Court of Appeal dismisses the claims from the Privacy First foundation.

Privacy First, a foundation that stands up for the privacy of Dutch citizens, appealed against the judgment of the court in preliminary relief proceedings. The foundation demanded a – preliminary – suspension of the Dutch legislation, as it was allegedly contrary to the right of privacy and protection of personal data. The court in preliminary relief proceedings ruled on 18 March 2021 that the obligation to provide the data of the Ultimate Beneficial Owners (UBO's) may not be suspended as the Dutch State may not act contrary to the fifth European Anti-Money Laundering Directive - AMLD5 -. We already issued a press release on this topic by mid-2021. Although it could not be excluded that the public character of the UBO register does not relate to principle of proportionality, the court in preliminary relief proceedings is of the opinion that a decision on the lawfulness of the AMLD5 Directive is reserved to the Court of Justice of the European Union.

The Court of Appeal in The Hague came to the same decision. The Court of Appeal held that Privacy First has not made it plausible that Ultimate Beneficial Owners would suffer serious damage in the short term. The foregoing is a requirement pursuant to the European directives to be able to – provisionally – suspend the UBO register. The Court of Appeal also took in consideration that an Ultimate Beneficial Owner who fears that due to the publishing of his personal data, he would run the risk of being abducted or extorted or something like that, could immediately protect his data from the general public. Dutch legislation already provides for such a possibility.

In September 2020, legislation which concerns AMLD5 has come into force in the Netherlands. The legislation concerned stipulates matters including the fact that companies must enter into the Trade Register who are their Ultimate Beneficial Owners (UBO's). In this context, UBO's are defined as the natural persons who are the ultimate owners. In addition, a number of personal data of these UBO's has to be provided, as well as the nature and the extent of the economic interest they hold. In principle, anyone can consult the UBO register to find out who the Ultimate Beneficial Owner is. Certain data, such as the address, the citizen service number, and the date and place of birth must be provided but such data are only available to institutions such as the Tax Authorities.

Incidentally, the Court of Appeal in The Hague does not see any reason to put prejudicial questions in respect of the UBO register to the European Court of Justice due to the fact a Luxembourg court has already asked questions. A ruling from the highest European court is expected by mid-2022.

Colofon

Redactie:

mr. Dorine Stahlie	Coördinator kennis & expertise
mr. Ruut Regtering	AML specialist
mr. Joris Rozemeijer	AML specialist
drs. Erik Reissenweber	AML specialist
mr. Michael Schmitz	AML specialist

Anti Money Laundering Centre
Utrechtseweg 297 gebouw C, 3731 GA De Bilt

www.AMLC.nl
www.AMLC.eu

E: AML.Centre_Postbus@belastingdienst.nl

To subscribe or unsubscribe, please send an email

ANTI MONEY LAUNDERING CENTRE