AMLC

Newsletter november 2021

Anti Money Laudering Centre

Dear Colleague,

Last month we were again confronted with leaked records from consulting firms that set up companies in tax havens: the Pandora Papers. Another leak; it doesn't even scare us anymore. Once again this makes it painfully clear how much wealth is being hidden. Of course, the AMLC is looking for relevant money laundering signals and knowledge about the constructions used.

Such a leak also forces us to examine whether we are doing the right things, and whether we are sufficiently connected with our cooperation partners. A first step is to share knowledge. So, if you have experiences or constructions that you would like to share, please mail to AML.Centre_Postbus@belastingdienst.nl.

This newsletter contains a number of reading and listening tips, attention for the new reporting group for remote gambling providers, and an article based on our analyses of suspicious transactions. As always, we conclude with case law.

If you have gained experience or have run into set-ups that you want to share, please mail AML.Centre_Postbus@belastingdienst.nl. Do you know any colleagues who would also like to receive the newsletter? They can subscribe using this email address. Lastly, if you want to stay up-to-date: follow us on LinkedIn!

Enjoy the read,

The AMLC

ANTI MONEY LAUNDERING CENTRE

News

Reading tip: Coda Oligarchy, a blog by Oliver Bullough
You may be familiar with the book 'Moneyland' by Oliver Bullough. The well-known British investigative journalist and writer published the book in 2019. Oliver goes back to the history of the development of the offshore industry and he reveals how criminals and the super-rich manage to conceal hundreds of millions from the view of the government by way of shadowy financial structures.

But do you also know that Oliver Bullough continues to give regular new insights by way of a blog/newsletter? He tirelessly publishes matters in great detail such as:

- the reason why the impact of South Dakota's industry should be thought about critically (spoiler-alert: something to do with secrecy)
- How the Czech prime minister Andrej Babiš secretly spent 22 million dollars on a French castle;
- that politicians who boast about being anti-globalist also appear to be the most enthusiastic exploiters of the global financial system;

Oliver recently told readers of his blog during a virtual meeting about the Pandora Papers, and how it has again become obvious that the super-rich are using tax loopholes.

In his journalism, Oliver Bullough does not only enable policy makers to assess the risks more accurately, he also helps investigating officers and analysts who conduct transaction monitoring and KYC to do the same as Bullough explains the context of transactions and company structures clearly. Are your interested? Go to: https://www.codastory.com/coda-newsletters/.

New reporting group – Money Laundering and Terrorist Financing (Prevention) Act

As of 1 October 2021, the online gambling market has been opened in the Netherlands after the Distance Betting and Gaming Act came into force. At the beginning of October, ten companies obtained a licence from the Dutch Gaming Authority to offer online gambling in the Netherlands. In order to be considered for such a licence, the providers must meet requirements which concern consumer protection and addiction prevention and they must set up a monitoring data bank with near *real time* gaming data. In addition, the providers now come within the scope of the Money Laundering and Terrorist Financing (Prevention) Act. They must conduct proper client screening and they must monitor the players and the transactions. In the guideline for the Money Laundering and Terrorist Financing (Prevention) Act in respect of the betting and gaming sector, reference is made to objective and subjective indicators which might give reference points for the reporting of unusual transactions. An objective indicator being a payment transfer transaction of an amount of € 15,000 or more. Click here for an update of our fact sheet: online gambling as a money laundering method and for more information from FIU-NL click here.

Join our game!
Would your company inadvertently become involved in a money laundering scheme? The Anti Money Laundering Centre (AMLC) developed a workshop together with PwC to increase knowledge and awareness of money laundering. Under the supervision of a data analyst and an anti-money laundering expert, you will investigate in groups how the fictitious *Nabook.com* is being misused to launder the proceeds of crime. You will learn more about money laundering and how to tackle a large amount of data. Are you working in compliance, integrity, Anti-Money Laundering or investigative practice? Preferably outside the financial sector? Sign up! Starting in December, every third Thursday of the month at locations all over the Netherlands. For more information click here.

New AMLC podcast
If you are acting as a financial institution or if you are trading as another company with China or if you are working as an investigative officer in an investigation procedure in which a Chinese company is involved in a transaction, it is good to know what risks of money laundering the FATF records in their assessments. You can read the FATF's reports with this in mind. FATF published a follow-up report about China this month. You can also listen to the 15 minutes AMLC podcast in which our colleague Anne Strijker keeps you up to date. You can find it in your favourite podcast app!

Feedback in respect of suspicious transactions

By: Joris Rozemeijer, AML Specialist at AMLC

Introduction
The aim of the obligation to report unusual transactions is twofold: the prevention of misuse of the financial system for money laundering and combating money laundering[1]. The obligation to report is a matter of time and money to those institutions. Such commitment will avoid the misuse of the financial system in a preventive manner. But what is the contribution to the combating of money laundering from the point of view of criminal investigations? It makes sense and it is a sign of involvement that there is a call for feedback on what exactly happens to the unusual transactions as reported to the FIU. Various chain partners already provide such feedback. The FIU provides feedback in their annual overview[2] and their website contains casuistry[3] in which suspicious transactions have played a role.
The Supervisory Authorities[4] pursuant to the Money Laundering and Terrorist Financing (Prevention) Act (*Wet ter voorkoming van witwassen en financiering van terrrorisme* or Wwft) are naturally important against this backdrop. These authorities do not actually receive any unusual transactions but they do provide guidance to the institutions that have the obligation to report transactions and to clarify what must be reported to the FIU. Apart from providing guidance, they may also act under administrative law.

The Anti Money Laundering Centre (AMLC) intends to make a contribution to feedback in this article, by reflecting on the details of the suspicious transactions as viewed in the quarterly report of the AMLC. As

[1] TK 1992-1993, 23 009, nr. 3 pag. 2
[2] fiu-nederland jaaroverzichten
[3] fiu-nederland casuistiek
[4] Art. 1d Wwft

AMLC draws up several analyses, and one of these is the quarterly report which contains an analysis of suspicious transactions for the purposes of criminal investigations: what are the highlights, what are the opportunities and what are the bottlenecks from a law enforcement perspective?

This contribution initially contains considerations on barriers in giving feedback from law enforcement perspective. Subsequently, suspicious transactions of crypto companies are considered in detail. In the most recent quarterly report (Q2 2021), it is striking that the number of suspect transactions from crypto companies has risen by 80% compared to the previous quarter. In the future, other conspicuous items from our analyses will be explored in detail.

Barriers and opportunities

The feedback on unusual transactions in the public domain is full of barriers and it mainly is a search for opportunities. First of all, it is only the Financial Intelligence Unit that has a view of all of the unusual transactions. After analysis by the FIU, part of the transactions is set forth as being suspicious transactions which are subsequently made available to law enforcement officers such as the ones from the Police and the Fiscal Intelligence and investigation Service (*Fiscale inlichtingen- en opsporingsdienst* or FIOD). The AMLC (with mainly FIOD staff) can only reflect on suspicious transactions and not on unusual transactions. The 2020 annual report from the FIU shows that out of 722.247 unusual transactions, 103.947 were found to be suspicious transactions. In addition, the annual report also contains a description of the four ways in which unusual transactions become suspect transactions: by way of investigations conducted by FIU itself, by way of hits using data from the index named Reference Index Criminal Investigations and Subjects (*Verwijzingsindex Recherche Onderzoeken en Subjecten* or VROS), by way of hits using data from the Central Judicial Collection Agency (*Centraal Justitieel Incasso Bureau* or CJIB) and by hits with National AML Public Prosecutor – requests (*LOvJ-verzoeken*).

A further barrier is the confidentiality of criminal investigations and the limited way in which criminal judgments show the use of suspicious transactions. Let us suppose that a suspicious transaction gives cause for a criminal investigation or it supplements an ongoing criminal investigation. Nobody would know except for the investigating officers involved and the Public Prosecutor charged with the investigation. The moment it is first publicly revealed is the date of the actual hearing of the case before the court. It remains to be seen if during the course of that court hearing, it is revealed that specific information comes from a suspicious transaction. As a rule, during the course of an criminal investigation, financial information is gathered on different occasions and in the court hearing, the modus operandi tends to be specifically scrutinized by considering what exactly happened and/or whether it results in an act which is provable; generally, the question as to how the information was obtained is not considered or considered to a lesser extent. It comes down to the fact that via published case law it is not possible to get an exhaustive overview of judgments of cases in which suspicious transactions played a part. Another aspect is that those who report unusual transactions are not happy that reference is made to them in a criminal case; at times it is clear that the report must have been filed by X, Y or Z, however the Public Prosecutor prefers not to focus on who reported a transaction.

The confidentiality of unusual transactions or suspect transactions can be found in various sections of the law. The provisions that concern confidentiality and secrecy are there for reporting entities, the supervising authorities, the Financial intelligence Unit and law enforcement. The relevant provisions are

mainly found in Money Laundering and Terrorist Financing (Prevention) Act (Wwft) and the Police Data Act (*Wet Politiegegevens* or WPG). The statutory provisions stipulate that feedback from the AMLC may not contain personal data and/or may not be traceable to a person. The consequence is that suspicious transactions are described with a certain amount of abstraction and shown in a larger context, it is in fact almost impossible to focus in on a particular suspicious transaction without a transaction being traceable to a person. Even if the government would like to stress how important unusual transactions are, it is often simply not possible. This might not be satisfactory for some reporting entities.

Feedback on suspicious transactions, crypto companies

The large increase in suspect transactions of crypto companies in the second quarter of 2021 (as referred to before, a rise of 80% by comparison to the first quarter of 2021). Crypto companies are defined as exchange services in virtual currency and providers of crypto wallets[5]. The crypto companies comprised 7.7% of the suspicious transactions in the second quarter. The obligation to register and to report on the part of the crypto companies is relatively recent (as of 21 May 2020 pursuant to the Money Laundering and Terrorist Financing (Prevention) Act (Wwft) and the increase of in reported transactions are in line with what might be expected from these new reporting entities. It is especially so as cryptos may be interesting to criminals. A judge of the criminal court formulated it in his judgment[6] as follows "it is a well-known fact that bitcoins are often used in criminal environments, including drug trafficking." In view of the current development and the legalization of the branch via the Money Laundering and Terrorist Financing (Prevention) Act (Wwft), it seems that this well-known fact is rather bold now and it does not do justice to the legal users of crypto services. A more balanced view can be seen on the Internet site of The Dutch National Bank (*De Nederlandsche Bank* or DNB)[7]; Cryptos are vulnerable to financial and economic crime". Crypto services have an increased risk[8] for being used by criminals as a result of which there might be a reasons to report an unusual transaction earlier. A positive development in this area is that part of the crypto companies is registered at the Dutch National Bank (DNB)[9], they are under the supervision of DNB and they report to the FIU.

In exact figures, 921 suspect transactions come from 12 different exchange services in virtual currency in the quarter as analysed. The aforementioned suspicious transactions amount to € 17,499,877. 375 suspicious transactions are from providers of wallets, amounting to € 6,742,336. The relationship between the transactions reported on an objective indicator and a subjective indicator is fifty-fifty. The Appendix 1 of the implementation decree of the Money Laundering and Terrorist Financing (Prevention) Act (Wwft)[10] includes that the objective indicator applies to transactions of € 15,000 or more or for exchanging a virtual value to a cash value of € 10,000 or more. The identification of transactions on the basis of such objective indicators is quite straight forward. In the implementation policy, the subjective indicator is considered to possibly be linked to money laundering and the financing of terrorism. The guideline from the DNB pursuant to the Money Laundering and Terrorist Financing (Prevention) Act (*Wwft*) and the Sanctions Act [11] has not been finalized for crypto companies. DNB refers[12] on its website to the FIU[13] website for more information about the subjective indicator. The referral to the FIU results in a list of typologies from 2017 in relation to the buying and selling of virtual payment instruments. The FIU

[5] Art. 1a lid 4 sub l & sub m Wwft
[6] ECLI:NL:RBROT:2019:2408
[7] DNB integriteitstoezicht op aanbieders van cryptodiensten
[8] Zie ook deze infographic n.a.v. het NRA
[9] DNB registers van aanbieders van cryptodiensten
[10] uitvoeringsbesluit Wwft 2018
[11] DNB leidraad wwft en sw (zie p.5/p.6)
[12] DNB indicatoren die bij cryptodiensten kunnen wijzen op ongebruikelijke transacties
[13] fiu-nederland witwastypologieen virtuele-betaalmiddelen

also refers to a list[14] of countries that are considered to be an increased risk. The identification of transactions based on the subjective indicator is less straight forward and needs a tailored approach.

Upon analysis of the suspicious transactions by the AMLC, and it is very likely to apply to other law enforcement agencies, that the 'reporting text' is the first thing that is looked at. The explanation that reporting entities provide, or as the provisions of the Money Laundering and Terrorist Financing (Prevention) Act (*Wwft*) stipulate the description on the basis of which a transaction is designated to be an unusual transaction[15], is of great relevance in order to ensure that a suspicious transaction is upgraded to a criminal investigation. Without having a fully-fledged disclosure text, any suspicious transactions are generally more of a database at the service of ongoing criminal investigations rather than a starting point for criminal investigations. Equally, such a database is valuable and it provides an insight into the identity of a person who is behind the receiving wallet; unfortunately, so far, where suspicious transactions are concerned, it is seldom known who the person is behind the sending wallet.

For the benefit of this article, the reporting texts of the crypto companies have been examined in detail. It is conspicuous that from the transactions that were reported on a subjective indicator in the quarter as analysed, 80 % of the suspicious transactions only include a receiving wallet and/or a transaction code. The remaining 20% of the suspicious transactions also set out coded/standard reporting texts, the most frequently occurring texts refer to the darknet market, a presumption of a connected transaction, broker scams and child abuse. There is only 1% of the suspicious transactions which involves a 'unique reporting text'; in such cases reference is made to websites or companies. Such specific statements are indeed links which are necessary for investigations in order to be able to act on a reported transaction. With a view to the future of such suspicious transactions and their usability, it is useful for the purpose of investigation if more of the reporting texts consist of unique texts, possibly with an appendix. It is a regular incidence to see a coded disclosure text which shows that the compliance department noted an unusual transaction without any further 'unique reporting text' as to why the compliance department came to such a conclusion. In the event that a compliance department would provide such an explanation, investigations might be provided with leverage to be able to proceed with a suspicious transaction. The fact that specific websites or companies are named are good examples, however, overall, it is a matter of elaboration on the unusualness of the transaction which helps an criminal investigation on its way.

All of the transactions which are over the limit of the objective indicator are presented as an 'objective report'. No subjective transactions were reported which are higher than the limit of the objective indicator. It seems a natural outcome of the indicator system we have in The Netherlands. The customization needed for reporting an subjective transactions is not necessary for the objective indicator, whilst it is especially valuable to law enforcement to know if (especially for the higher amounts) in addition to the objective indicator, there is also a subjective indicator. It is therefore not surprising

[14] gedelegeerde verordening EU van 14 juli 2016
[15] Art. 16 lid 2 sub e Wwft

to note that in the cases of suspicious transactions which have been reported on the basis of the objective indicator, there are hardly any 'unique reporting texts'. The foregoing while the top objective transactions represent a value between two hundred thousand and three hundred thousand Euros and it is particularly relevant to the transactions representing a higher value that explanations are given on the unusualness.

In conclusion
All of the unusual and suspicious transactions reported by crypto companies have made it possible for the government authorities to be able to have a view of the money flows that may imply crime and to investigate underlying criminal offences.[16] In almost all financial criminal investigations it will be investigated if the FIU has suspicious transactions. Some suspicious transactions or groups of suspicious transactions may be used as intelligence or may evolve into a criminal suspicion and form the starting point for a criminal investigation. The reports from the crypto companies have made a contribution to the above. The value to law enforcement might even have more substance if the unusual transactions reported on an objective indicator and a subjective indicator contain more unique reporting texts that specify why the transaction is unusual. Hopefully this feedback provides some inspiration to achieve this objective.

Case law

District Court Amsterdam, 1 September 2021, banking relationship – charity foundation ECLI:NL:RBAMS:2021:4667

This case concerns the issue as to whether the Rabobank was allowed to terminate the banking relationship with a charitable foundation for Palestinian orphans in Gaza, Lebanon and Turkey. The bank terminated the banking relationship as it was unable to establish the origin and the destination of the flow of money. The bank alleged that the foundation had taken over activities from another foundation which might possibly support terrorism. On several occasions, the bank requested a certification which monitors that a charity actually contributes to a better world as well as carefully managing their expenses. Such a certification requires an audit report from an accountant. In addition to the requirement of a certification, the bank requested an internal compliance policy. Eventually, the foundation obtained the audit report on 31 March 2021. The foundation has no certification – as yet.

As far as the issue is concerned whether it was allowed to terminate the banking relationship, the court in preliminary relief proceedings considered it relevant that two members of the board of the foundation, who were relatively new, made arrangements for a reputable office to conduct an audit of their financial statements. They furthermore were actively in the process of obtaining the certification. In addition, it is of importance that the foundation sent lists of orphans, proofs of payments and copies of passports to

[16] Zie vice versa ECLI:NL:RBAMS:2021:2600 e.a.

the bank and that the bank did not indicate that anything was wrong or missing. The bank had certain ideas as to what the compliance policy of the foundation should entail but the court states that it is unclear what such a policy should involve and what the benefit would be. The bank did not clarify this. The foundation submitted its reasons as to why it knows exactly where the money ends up (i.e., it is going to the orphans). The foregoing was verified by an accountant by way of a statement added to the annual financial statements. In addition, the submission of the audit report and the quality certification have taken longer due to the corona pandemic. On the bases of the foregoing, the court is of the opinion that there are too few indications that the working method of the foundation is contrary to the Money Laundering and Terrorist Financing Act (*Wet ter voorkoming van Witwassen en Financiering van Terrorisme* or Wwft) and other relevant acts and as a result. The bank must continue the relationship.
The concerns and the alertness of the bank in respect of the risks of money laundering and the financing of terrorism in this case are with very good reason. In order to make an assessment, the court considers it important that the foundation provided evidence of the destination of the money and that it was approved by an accountant.

The court in the first instance of Curaçao, 14 September 2021, Embezzlement and money laundering by a civil-law notary: ECLI:NL:OGEAC:2021:161
This case concerns a civil-law notary in Curaçao who is suspected of the embezzlement and money laundering of 1.4 million Antillean Guilders (converted approximately € 670,000) via the clients' account of his office over a period of ten years. He effected the same by diverting funds from the clients' account via his mother's bank account to his personal bank account. He subsequently used this money for buying a piece of land and luxury goods such as a car and a piano. The suspect concealed the fact that it was money that was withdrawn from the clients' account by giving these transactions incorrect descriptions such as a "loan" or an "immovable property transaction". The suspect was also aware that the amounts were coming from the clients' account and that the money did not belong to him, but to third parties. By concealing the money from the person entitled and to embezzle it and to withdraw the money afterwards and to convert it, the suspect concealed the criminal origin of the money and is guilty of money laundering. As a result of the long duration and the frequency, the court sentenced the civil-law notary on account of habitual money laundering and also on account of embezzlement as a civil servant.

As the suspect has been living off the money, he converted it. It counts strongly against him that he abused his position as a civil-law notary. It is for that reason that he was sentenced to a term of imprisonment of 1.5 years, a disqualification from his profession and confiscation proceedings will follow. In the Netherlands a conviction for money laundering during the course of practising a profession would be self-evident but a sentence-increasing provision is not or not yet part of the penal law in Curaçao.

The Trade and Industry Appeal Tribunal, 7 September 2021, the right to remain silent of an accountant:ECLI:NL:CBB:2021:857
In these disciplinary proceedings the Public Prosecution Service (*Openbaar Ministerie* or OM) filed a complaint against an accountant on account of wrongfully providing an audit certificate of approval and not reporting unusual transactions in good time to the Financial Intelligence Unit (FIU). In the proceedings at the Accountancy Division, the accountant did not put up a substantive defence, on account of the fear that his statement in the disciplinary hearing might be used against him in his criminal case. According to the Accounting Division, the accountant was free not to put forward a substantive defence, but it did not alter the fact that he did not contest the accusations. The complaint from the Public Prosecution Service was subsequently upheld in all its components.[17] On appeal, the

[17] Due to a substantial and structural flow of money without invoices or contractual obligations in writing, a loan to a Director and a loan to another entity without the provision of security, the accountant should have seen reasons to report to the Financial Intelligence Unit (FIU). In addition, there failed to be a reliable base for the audit reports as issued.

accountant argued that he was sentenced twice for the same act, as the penal law provides for the same sanction in the form of a disqualification from a profession as disciplinary proceedings do in the form of deregistration. The accountant argues that the Public Prosecution Service bypasses the nemo tenetur principle by filing a disciplinary complaint. The tribunal stated that the Public Prosecution Service recognized that during the course of a concurrence between penal and disciplinary proceedings, an accountant may come into conflict with the nemo tenetur principle as applicable in penal law. Further to the fear of the accountant to break his right to remain silent if he would conduct a defence in the disciplinary proceedings, the Public Prosecution Service declared in a letter that the statement would not be submitted in the penal case. The Tribunal considered the foregoing insufficient as the letter only ensured that statements in the disciplinary proceedings were not added to the ongoing criminal proceedings. Not until the court hearing on appeal did the Public Prosecution Service make an unequivocal undertaking that the decisions in the disciplinary proceedings would not be added to the records of the criminal case. Further to the foregoing, the accountant indicated that he was prepared to make a statement in the disciplinary proceedings. The Tribunal is of the opinion that the accountant must be given said opportunity and it refers the case to the Accounting Division.

The nemo tenetur principle means that a suspect in a criminal case may not be forced to cooperate in his own conviction. This principal only applies if it is a matter of a criminal charge within the meaning of Article 6 of the European Treaty for the Protection of Human Rights and Fundamental Freedoms which is not at issue here. The concurrence between penal law and disciplinary law is acceptable. Even if the Public Prosecution Service filed a disciplinary complaint. It is not a matter of bypassing the nemo tenetur principle, but on account of the dispute that has arisen in respect of said penal principle, the unequivocal undertaking on the part of the Public Prosecution Service stating that the statements will not be included in the criminal file is obviously in place.

Colofon

mr. Dorine Stahlie
mr. Sophie de Ridder
mr. Ruut Regtering
mr. Joris Rozemeijer
drs. Erik Reissenweber

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