AMLC

Newsletter March 2022

Anti Money Laundering Centre

Dear colleague,

Here we present a new AMLC newsletter about developments in the area of combating money laundering.

In this newsletter we share links to several new AMLC products, including an overview with money laundering risks of offshore companies in relation to (real estate in) the Netherlands. More products can be found under knowledge products.

Furthermore, a feedback regarding reported (and declared suspicious) transactions with real estate as the object of the transaction, and an article based on learning experiences of crypto exchange LiteBit. If, like LiteBit, you have had experiences or encountered constructions that you would like to share, please do! Please email AML.Centre_Postbus@belastingdienst.nl.

As usual, we finish off with case law, this time concerning judgments relating to a rental estate agent who received rent in cash, the provision to a bank of data relating to donations by a client, and the termination of a bank relationship with a trust office.

If you have had experiences yourself or you have come across constructions which you would like to share, then send an email to AML.Centre_Postbus@belastingdienst.nl. If you know of any colleagues who would also like to receive our newsletter, then they can request that via the same email address. And finally, if you want to keep up-to-date: follow us on LinkedIn!

Enjoy the articles,

The AMLC

ANTI MONEY LAUNDERING CENTRE

Knowledge products

Risk indicators offshore companies

The AMLC offshore companies project is aimed at mapping out the money laundering risks of offshore companies in relation to the Netherlands. Offshore companies are mentioned as a major money laundering threat to the Netherlands. Given all publications concerning the investment of criminal money in real estate, this is the first priority. In the recent period, the project investigated offshore companies that purchased property in the Netherlands. This has led to concrete signals, but also to an overview of characteristics of those signals, which are described as risk indicators. The document can be found here (only in Dutch!).

By offshore company is meant a foreign legal entity established and registered in a risk country. Although not forbidden in principle, the holding of real estate by offshore companies in this country offers many opportunities for criminals and fraudsters to invest assets from criminal sources and to benefit from this investment or make a return on it.

NFT's

Our colleagues from the FIOD Financial Advanced Cyber Team made a very nice knowledge product about Non-Fungible Tokens. What are NFTs, how do they work, and how can they be used for money laundering? Dive into the NFT world here (only in Dutch).

Risk indicators virtual currencies

Virtual currencies are regularly associated with money laundering. But what behaviour offers clues to money laundering with virtual currencies? The Europol Financial Intelligence Public Private Partnership (EFIPPP), established in 2017, is an international partnership for information sharing in the fight against, among other things, money laundering. In this form of consultation, representatives of Financial Institutions, Financial Intelligence Units and investigative bodies exchange information among themselves regarding observed money laundering phenomena. Recently, the EFIPPP shared a document with red flags around the use of virtual currencies. We have made this list of indicators available via our website with some minor adjustments. They may be useful for application in systems and procedures to effectively detect financial crime. The overview can be found here.

Modus operandi alert: the crypto money mule

By: Lisa Tevel (LiteBit) and Erik Reissenweber (AMLC)

In the case described in this article, a fraudster uses a money mule, among other things, in order to conceal the origin the assets acquired from fraud and keep a low profile with regard to the authorities. We explain in this article how the money mule is deployed and which route the criminal takes within the financial system. Since money mules frequently continue to play an important role for fraudsters, we offer some guidelines for recognising similar situations, so that these practices can be stopped at an earlier stage.

Blocked crypto transactions bring fraud to light

In the spring of 2021, several unusual transactions were blocked by LiteBit. The transactions did not match the client profile drawn up previously by LiteBit. Subsequently, an employee at LiteBit's customer services department received a remarkable telephone call. An unknown person asked if, *in their position as LiteBit employee*, they could say why his Bitcoin transaction had been stopped. What was going on here?

As a result, a customer service representative received a remarkable phone call. An unknown person asked why his bitcoin transaction was being held up, even though he was a LiteBit employee. What was going on here?

The crypto money mule received online training

A fraudster placed advertisements on social media: "make money fast at home!". Of course, that sounds very attractive. A potential money mule (22) responded via Instagram and was redirected to what appeared to be the trustworthy website of a company where he filled in his details in a job application form. Soon afterwards, during a virtual meeting, it was explained to him by an English-speaking manager what was expected of him and, after signing what looked like a professional employment agreement, the money mule could begin.

This money mule was given the assignment to test payment systems, including those used by LiteBit, while LiteBit was completely unaware of this. In doing so, he would receive bank payments from so-called colleagues paid into his bank account. He was to convert the amounts received into crypto in accounts made by him with various crypto companies. As soon as those Bitcoins were placed in his Bitcoin wallets, he was instructed to transfer those Bitcoins to an external Bitcoin address of which he had been given sufficient details. He was allowed to withhold an agreed fee on his bank account and in this way he quickly earned money for himself.

In the case of Bitcoin transactions, there is no name-number check as used by banks and so it was impossible for the money mule to see who the owner was of the external Bitcoin address to which he sent Bitcoins. During the training, the money mule also learned how he could respond to any difficult questions he might elicit from his bank. There were, for example, the existing fake Marktplaats

advertisements that could demonstrate the origin of the assets, which can be designated as legitimisation, being one of the phases of money laundering.

Incoming payments originating from fraud
At the same time, the fraudster placed expensive TVs in a web shop at attractive prices. Interested buyers placed orders and paid in advance, using a normal and non-reversable bank transfer to a bank account cited in the order confirmation email. Needless to say, the TVs were never delivered. Instead, the money was received by the money mule onto his account, which he then converted into Bitcoins according to the aforementioned instructions.

Concealment of money acquired criminally - modus operandi
In doing so the money mule is suspected to have been involved in laundering criminally obtained money. This is a serious offence punishable by imprisonment. Especially if the money mule knew that the money was criminal money, among other things, the instructions on how to deal with difficult questions from the bank may indicate this.

Through paid crypto analysis tools, such as Elliptic or Chainalysis, it is possible to find out where the crypto comes from and what its final destination is, for example a darknet market wallet address. Certainly not all companies subject to the Wwft obligation make use of this type of analysis tools. Via www.blockchain.com (choose 'Explorer' on this website and enter hash or wallet address) and on the basis of a crypto trade history of the client, one can gain insight into the BTC transactions carried out. The openness also makes it possible for e.g. bank employees to verify the customer's statement.

Another website which can be deployed as a tool is: https://scam-alert.io/. The website provides insight into which wallet addresses are used for fraudulent or illegal activities. Be aware, however, that a wallet address can be made quickly and easily, and that it does not necessarily mean that a wallet address is not fraudulent if this is not stated.

The fraudster can also choose to send the cryptos to an exchange, possibly a foreign one, convert the coins into another type of crypto (sometimes known as chain-hopping) and then forward the amount. This is done in order to send anyone tracking the matter down the wrong path and to conceal the criminal origin of the money. However, a risk still remains for the fraudster when chain-hopping cryptos. A digital footprint is left after every exchange, such as login details, even if the KYC requirements are not taken fully into account.

Modus operandi of this crypto money mules case
As happens all too often in this type of case, many institutions are involved in the fraudulent practice and not any of the parties involved has a full view of the money flow. The following habits can be identified from this case, which may help to detect money laundering:

- For banks: deviations from expected transaction patterns
    - Unexpected large amounts are received from different accounts into an account into which normally speaking only student grants or monthly payments for part-time jobs are paid;
    - Approximately the same amounts are transferred to unknown accounts and, in this case, crypto platforms, after deduction of proportionally the same amounts, then that is another indication that the account holder may have been recruited as money mule.
- For crypto platforms: deviations in expected transaction patterns
    - In this case, LiteBit saw a sudden and unusual increase in volumes and numbers of transactions;

    - Purchase of Bitcoins that are immediately transferred to external addresses may be reason for further investigation;
    - Transfers to Bitcoin addresses which can be linked to mixer services, darknet or criminal activities also deserve attention.
- For payment institutions: deviations relating to online web shops
    - The sudden appearance on a web shop of offers which seem almost too good to be true, then the offers may well be just that. Sometimes the payment institution can temporarily postpone the payment to the new business, so that any complaints arising about deliveries can be resolved before the owner has disappeared with the loot.

Sharing modus operandi in the fight against money laundering

In the event of inexplicable unusual transaction behaviour, it is of course important to ask the relevant client about the purpose and nature of the crypto transactions, and possibly who the owner is of the external wallets to which the crypto is transferred. It seems likely, when coming across such transaction behaviour, that a bank can quickly find out whether this involves money mule activities, certainly if the client is questioned and despite all the clever training the money mule received.

This article was produced through a public-private collaboration. Lisa Tevel, who is employed by LiteBit, approached the AMLC and was prepared to share this casuistry in the hope and expectation that other market parties will also gain some advantage in combating financial economic crime. Our appeal is therefore not only to share and circulate the modus operandi to AML/CDD departments, but also other departments such as customer services of parties which fall under the obligations of the Money Laundering and Terrorist Financing (Prevention) Act. We believe that it is possible to pick up on signs and red flags at an early stage. We hope that we have been able to make a contribution to that through the publication of this case.

Feedback over Suspicious transactions

Real estate as object of the transaction

By: Joris Rozemeijer (AMLC) in collaboration with FIU-Nederland

What is remarkable is that, during the fourth quarter of 2021, the number of suspicious transactions with real estate as object increased by 174% in comparison with the third quarter[1]. This interesting development provides reason to take a closer look in this article at these suspicious transactions.

[1] AMLC Quarterly report Suspicious Transactions 2021 Q4

The aforementioned increase of 174% is a good development, representing in absolute figures 52 items of real estate, 46 transactions and 34 persons reporting. However, this if far from the only data reported concerning real estate, although these reports have no money flow as object but real estate instead. From a search through the text in all the suspicious transactions in Q4, therefore also the suspicious transactions related to a money flow, it appears that 1.3% of all suspicious transactions concern real estate.[2] In this article, focus is placed on the suspicious transactions involving real estate.

Besides cars and jewellery, real estate is one of the classic final destinations of money laundering. Second houses or real estate portfolios provide the perfect nest egg, they can even deliver a subsequent profit through rental income and, moreover, a holiday cottage is fun for holidays. Added to that, there is a great deal of legal money involved in real estate and valuations can vary greatly and then the money laundering risks become visible. That this involves large amounts in real estate is evident from the aforementioned 46 suspicious transactions, 9 of which concern suspicious transactions involving an amount of more than one million euros. Both internationally and nationally, real estate and money laundering is a topic which regularly attracts attention. Internationally speaking, there are typology reports from the FATF, for example, and various other studies carried out, for example, by the OECD, the Egmont Group and the European Parliament.[3]

Attention is being paid nationally as well in all sorts of ways to real estate and the reporting system. A report has been produced, for example, about the willingness to report amongst estate agents[4] and a report about the collaboration between civil-law notaries, estate agents/valuers and government institutions for the prevention of money laundering and fraud in real estate transactions.[5] The letter to the House of Representatives from the Minister of Justice and Security is also worthy of note.[6] Under the scope of the progress in combating undermining crime, commitments are made in that letter which offer further safeguards for the safety of the person reporting an unusual transaction. If an unusual transaction from a small business becomes a suspicious transaction and is subsequently used as evidence in a criminal file, then the detection services will contact that person reporting in order to find out whether any risks of threat exist. Developments can also be seen at the FIU which are helping to improve the reporting system including, for example, a simplified reporting form that has been developed for civil-law notaries.[7]

The 34 persons reporting suspicious transactions with real estate as object are mainly civil-law notaries, followed by estate agents, plus the occasional one reported by accountants, lawyers, banks and tax advisers. The quality of the reports from civil-law notaries is generally praised by the assessors of suspicious transactions in the criminal law chain. This is partly due to the excellent information position of the civil-law notary, through which a solid image is often sketched from A to Z of what is actually going on. It was good to see that, within this small group of 46 suspicious transactions, clusters were detectable. It was possible to see, for example, that in 4 of these 46 suspicious transactions the same business crops up in a dubious role.

[2] Total number of suspicious transactions in Q4 2021 is 23,655, 1.3% is 316 suspicious transactions
[3] For example: FATF/Egmont Group, Concealment of Beneficial Ownership, 2018; and; European Parliament, Understanding money laundering through real estate transactions, 2019; and; OECD, Real estate sector: Tax fraud and money laundering vulnerabilities, 2007.
[4] Centre for crime prevention and security, Willingness to report by estate agents, 2020.
[5] Leading team Undermining, Together, Collaboration of civil-law notaries, estate agents/valuers and government institutions for the prevention of money laundering and fraud in real estate transactions, A.B. Hoogenboom, 2021
[6] House of Representatives, session year 2020-2021, 29 911, no. 292
[7] https://www.fiu-nederland.nl/nl/per-27-oktober-nieuw-meldformulier-voor-notarissen

The information position of estate agents is less financial in nature. Nevertheless, through the large amount of contact with the client, the estate agent is able to recognise indicators which another person, such as the civil-law notary, may not see. Report texts from civil-law notaries are often more financial in nature as well and are responsible for the 'source of fund' investigation, for example, or an ABC transaction while in the report text from an estate agent there are more often reports following 'bad press' or seizure of criminal assets. It is interesting to see that reports are also made when a business buyer enters into a real estate transaction while the private residence of that buyer is subject to seizure of criminal assets. It is likely that such reports are relevant for an ongoing confiscation proceedings.

A previous analysis carried out by the AMLC shows that estate agents often make reports because payments are made in cash, originate from foreign accounts or because clients wish to buy premises without a mortgage. But now the follow-up. The unusual transaction is deemed by the FIU-Nederland to be a suspicious transaction, but a suspicious transaction is not yet a criminal suspicion.[8] For a suspicion, facts or circumstances are needed which give rise to the reasonable suspicion of guilt of a punishable offence. Only once there is a suspicion then the judicial chain has greater power to be able to request further information. For example, the frequently used demand under Article 126nd of the Code of Criminal Procedure[9] by which, for example, bank statements, compliance files or other financial documents are demanded by financial institutions. Prior to a criminal suspicion, it is possible to look at other suspicious transactions, public sources and the detection agency's own sources, although a great deal of information remains unavailable because there is no suspicion yet bringing with it the associated powers.

The report texts in suspicious transactions describe the circumstances. In order to arrive at a suspicion, the detection services must supplement these circumstances with facts. Furthermore, the whole case must be linked to a punishable offence. Imagine now that there is a suspicious transaction because the buyer makes varying statements about the 'source of funds' to a service provider. In that case, it is very useful to add any emails or forms originating from this buyer, through which the latter is evident, to the report intended for the FIU. This augments a report with facts and it enables the detection services to arrive at a suspicion of forgery, for example. The possibility of being able to reach such a suspicion otherwise is limited because, without suspicion, such documents cannot be demanded.[10]

Included on the website of the FIU[11] is a wide-ranging casuistry with examples of cases in which suspicious transactions in respect of real estate led to criminal proceedings. Experience shows that cases can be acted on sooner for criminal proceedings if there are multiple suspicious transactions in respect of one object and/or subject only. Hence, much value is added when a civil-law notary, estate agent and accountant all make a report. In order to be able to see and to analyse such connections, the department Data & Analyse of the AMLC has developed the AMLC browser. Suspicious transactions concerning real estate are often used as an enrichment to the information in investigations into a subject which are already ongoing. Moreover, the detection services greatly value the report texts which include information about the

[8] Article 27 Code of Criminal Procedure
[9] Article 126nd Code of Criminal Procedure. The detection agency requests by means of an application for an official report for data in accordance with Article 126nd, which is then issued by the public prosecutor.
[10] The FIU, in accordance with Section 17 of the Money Laundering and Terrorist Financing (Prevention) Act, can question a person reporting during the phase of an unusual transaction, although this power can no longer be deployed once the possibility has arisen of a suspicious transaction.
[11] https://www.fiu-nederland.nl/nl/wetgeving/casuistiek

'source of funds' and, in the case of legal persons, the UBO. This is because the core of many detection investigations lies in acquiring an image of money flows and who can actually be connected with those.

Real estate and combating money laundering will for the time being remain on the agendas of those fighting crime. Even if it is only to provide some protection against the effect of criminal money driving up the prices of real estate during the current overheated real estate market. Suspicious transactions concerning real estate are important sources of information and provide the detection services with reference points from which to go further. The addition of financial documents to an unusual transaction by a reporting person is highly valuable, certainly when those documents provide facts for a potential punishable offence.

Case law

Amsterdam District Court, 25 November 2021, Estate agent/landlord of real estate: ECLI:NL:RBAMS:2021:6768

In this case, a money counter, a firearm and cash amounting to more than € 350,000 were found at a residence. The tenant of the residence was found guilty of laundering the money. The suspect in this case is an estate agent and landlord of the residence. He received the rent for this residence in cash (€ 2,000) every month, which he then paid into his bank account. The question arises whether the money paid to the suspect originates from a criminal offence and also whether the suspect knew or should have known that. The District Court found that there were suspicions of money laundering. The next question is whether the suspect made a concrete and verifiable statement to which the suspicion of money laundering could be attached. The suspect declared that the tenants had a wholesale business in textiles, but that he had seen no documents relating to the company or the income of the tenants. According to the District Court, this statement is not concrete and verifiable. Since there was a lack of any indication of the tenant's legal income, the District Court found that the money paid to the suspect must have originated from crime and that the suspect should have suspected this. The suspect had received several warnings about receiving cash payments and the risk of money laundering attached to that. In addition, it had been pointed out to him that he was required to investigate the tenant's income and he should have kept an administration listing the cash payments. Despite all the warnings, the suspect failed to do so. Since the suspect should have suspected that the money originated from a criminal offence, he was found guilty of debt money laundering.

This judgment shows that landlords/estate agents of real estate who receive rent in cash, without any clarity that the money originates from a legal source, risk being found guilty of (debt) money laundering. This judgment is in line with a previous judgment given by the Amsterdam Court of Appeal about the responsibility of a landlord in relation to cash payments for rent. Click here to read more about this on the website of the AMLC.

Amsterdam Court of Appeal, 28 December 2021: Interim relief proceedings: is the GDPR an impediment to providing information about cash donations to the bank? ECLI:NL:GHAMS:2021:4148

ABN AMRO has terminated a banking relationship with a foundation, which funds a mosque, among other things, and which generates income in the form of donations, some of which are in cash. When questioned by the bank, the foundation answered that the donations originated from various sources, including the members of its community who gave monthly donations, other mosques and collections made by third parties, and that larger cash donations could be the total revenue from a benefit activity. The foundation refused to provide any further details about the donations, appealing to the provisions of the GDPR. During interim relief proceedings, the Court of Appeal took as basic assumption that personal data must be processed in accordance with the GDPR and that the GDPR contains a special regime for the processing of personal data evidencing religious beliefs. However, the GDPR does not stop the foundation from indicating whether a donation comes from a person or agency and whether it concerns revenue from a benefit activity, stating the date. Nor does the GDPR stand in the way of providing information about agencies from which the foundation has received cash donations. The GDPR only relates to the processing of the personal data of natural persons and not of legal persons. In addition, according to the Court of Appeal, ABN AMRO did not have sufficient insight into the total scale of the assets of the foundation and the origins of those. According to the Court of Appeal, ABN AMRO could terminate the banking relationship with the foundation because the foundation provided insufficient cooperation with the client investigation, which meant that the bank could not fulfil its obligations under the Money Laundering and Terrorist Financing (Prevention) Act.

The parties must fulfil the requirements of the GDPR when processing personal data. This applies particularly to personal data evidencing religious beliefs. However, the GDPR does not stand in the way of providing information to a bank about legal persons and agencies from which the client has received cash. After all, the GDPR only relates to natural persons. However, it is a different matter when the data about a legal person lead to a natural person, such as in the event of a self-employed person.

Amsterdam District Court, 5 January 2022, Banking relationship with trust office: ECLI:NL:RBAMS:2022:42

ING decided in 2019 that it wanted to terminate the banking relationship with a small trust office because the bank was no longer prepared to accept the higher risks attached to the trust sector. In relation to this, the bank pointed to the investigation carried out by DNB which showed that some trust offices did not comply sufficiently with the rules. More specifically, the bank asserted that this involved a small trust office with insufficient knowledge and skill for dealing with the complex international structures behind target companies, also without a sound compliance officer and supervisory board or other supervisory body. The trust office contested this and said that it knows all of its clients because it is a relatively small organisation with short lines. The office carries out thorough investigations into who the UBO is and what the structure and the origin of the assets of the company are before going into business with them. Moreover, the trust office has had a compliance officer since 2009.

On the basis of weighing up the interests, the District Court came to the conclusion that the banking relationship must be continued. Such a termination would mean that the trust office would not be able to continue its business because other banks had now indicated that they would not open a bank account for the trust office, while there were no concrete indications that specifically this trust office represented an integrity risk for ING. This does not mean that this situation may not change in the future. No period was set by the District Court for the continuation of the banking relationship, as was requested by the trust office.

It is true that DNB is critical about the trust sector because the sector is regularly linked to tax evasion and money laundering. That is why ING has been attempting seriously to limit the provision of services to the trust sector since 2017[12], but in this case the court did not permit the termination of the banking relationship. However, the court explicitly indicated that this situation may be different in the future, for example due to concrete suspicions of money laundering or on account of social or political developments.

[12] https://fd.nl/beurs/1225206/ing-beperkt-dienstverlening-aan-trustkantoren-mqb2cadoMQCs

Colofon

Redactie:

mr. Dorine Stahlie	Coördinator kennis & expertise
mr. Ruut Regtering	AML specialist
mr. Joris Rozemeijer	AML specialist
drs. Erik Reissenweber	AML specialist
mr. Sophie de Ridder	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