AMLC

Newsletter July 2020

Anti Money Laundering Centre

Dear Colleague,

We are pleased to be sending you the newsletter for July 2020. Perhaps it's a bit earlier than 'bimonthly', but that's because the June 2020 newsletter was thematic without any current news items.

In this newsletter you'll find current developments about money laundering using private investment funds, the latest about the national risk assessment, and how to find the new AMLC podcasts (with an explanation of sham litigation). Most links and podcasts are in Dutch, but this is because you're reading a translation of our Dutch newsletter. There's also an in-depth article about Wirecard. Wirecard has already received a lot of attention in the press; but has it been sufficiently approached from the perspective of money laundering? Finally, we discuss two examples of the latest case law, one of our regular features.

A big 'thank you' to everyone who completed our questionnaire about the newsletter! In general, our readers are very satisfied with the newsletter, and that means that we are very satisfied too. We are certainly going to be exploring all your suggestions for substantive topics. And in the near future there will be some changes to the layout of the newsletter, taking into consideration our readers' desire for one printable document. As you can see, we immediately complied with the request for an English language version of the newsletter.

We are always happy to receive your questions and comments; just email them to AML.Centre_Postbus@belastingdienst.nl. Especially if you would like to make a contribution to the AMLC newsletter yourself. Do you know colleagues who would also like to receive the newsletter? They can register using this email address too.

We hope you enjoy reading the newsletter and wish you a very pleasant summer!

Kindest regards,
The AMLC

ANTI MONEY LAUNDERING CENTRE

News

Private Investment Funds
A recent hack of American law enforcement websites (BlueLeaks) turned up, among other things, a document exposing the use of hedge funds and private equity firms for the purpose of money laundering. In the document, the FBI is warned that existing anti-money laundering programmes in the US are wholly inadequate in detecting money laundering channelled through hedge funds and private equity firms. This has therefore now become an attractive method for money laundering huge sums. The FBI document can be found on the website of the OCCRP (Organized Crime and Corruption Reporting Project), and elsewhere.

In the Netherlands, investment institutions have been subjected to more intense scrutiny by the financial market authority AFM. The regulator recently said that it would start making sure such firms got their transaction monitoring and reporting compliance quickly up to speed.

Money Laundering National Risk Assessment (NRA)
In recent months, a progress letter on the national money laundering Plan of Approach (PvA) was sent to the lower house of the Dutch parliament. The progress letter provided an update on the current situation of the PvA launched last year, including the fact that the UBO (Ultimate Beneficial Owner) Register, which is now finally regulated by law, will go live on 27 September. The letter with annexes can be found here.

As is already known, two essential tasks of the PvA are identifying money laundering risks and analysing whether these risks are being sufficiently mitigated. To that end, the first National Risk Assessment (NRA) was drawn up in 2017. The second NRA has now been sent to the Dutch lower house as an annex with the PvA (find it here).

How are risks of money laundering identified? What exactly is involved? We are specifically looking for money laundering risks with *the highest potential for lasting impact*. First, a group of experts identifies threats of money laundering with the highest potential for lasting impact; one example of this is trust offices. Second, the estimated impact of these threats is rated on a scale of 1 to 100. Third, the resilience of the policy instruments dedicated to preventing and combatting money laundering are assessed; for example, evaluating the measures in the Trust Office Supervision Act of 2018. The *potential for lasting impact* is the impact of the threats remaining after assessing the preventive and/or mitigating effects of the policy instruments dedicated to countering these threats.

It should also be noted that the current NRA does not yet include mitigating measures enacted as law in 2020. Thus, for example, virtual currencies have a high potential of lasting impact, but the recently adopted AMLD5 legislation, which includes *inter alia* an obligation to report for cryptocurrency exchange businesses, does not yet appear among the countermeasures.

On the grounds of Article 2(c)(1) of the Money Laundering and Terrorism Financing (Prevention) Act (WWFT), financial institutions in the Netherlands subject to that law are obliged to incorporate the risks identified in the NRA in their risk policies.

AMLC Podcasts
Two important cornerstones of the AMLC are knowledge sharing and collaboration. With that in mind, we recently made a number of podcasts, which are a very effective way of disseminating knowledge. We want these podcasts to stimulate the listener to think more deeply about the subject, and to make connections. For instance, if this money laundering construction is possible, then what other constructions might be possible? Or if a criminal uses sham litigation to legitimate a transaction, then what are some other constructions that could be used to give a semblance of legitimacy?

You can find the first three podcasts about money laundering in the news, trade-based money laundering, and business typologies here.

Sham Litigation
By the way, what are sham litigations? These are ostensibly legal court cases launched for the purpose of concealing money laundering. Every year the Dutch courts are tied up adjudicating hundreds of cases that have little or nothing to do with the Netherlands, where dubious parties from Russia or Moldavia, for example, cross swords in trumped up proceedings. It may well be that there is some link to the Netherlands because a letterbox entity is registered here; it may also be that the parties simply have a contractual agreement to submit their disputes to the Dutch courts.

A legal judgment obtained in this way can be used to disguise money laundering: the parties act as if they have had a conflict, allowing the court to take a decision about payment of a settlement. The court's judgement is then used to legitimate the payment of criminal monies.

The Russian Laundromat
One of the prime examples of this actually took place in what's called 'the Russian laundromat', which made use of a Moldavian court. There were two English companies, and one company supposedly lent the other a large sum of money. Russian and Moldavian companies were appointed guarantors of the loan. All of a sudden there was some kind of dispute about the loan, and one company launched an action against the other before a court in Moldavia. The court confirmed that one company had to pay the other a certain sum of money. Funds were then transferred from the Russian companies, who acted as guarantors, to the English bank account of the other company. If that company's bank had asked any questions about the transaction, the court's judgment could have been produced as a legitimation of the transfer.

Source: OCCRP

Wirecard viewed from a money laundering perspective

Reflections on possible accounting fraud and money laundering constructions at Wirecard

By Dick Crijns, senior advisor AMLC

1. Background

During the last two weeks I have been regularly asked questions about potential fraud at Wirecard. I noticed that everyone mentions potential accounting fraud and possible market manipulation, but in response to the open ends, questions are also asked about relationships with money laundering. Despite the fact that there is still very little that is really clear regarding the nature and scope of what has happened at Wirecard, I can see the necessary references points for more fraud, as well as a potential role for Wirecard in a money laundering scheme. In response to these questions, in this article I wish to set out a number of main points regarding the frauds and present some important background information.

As far as I am concerned, this is an open end article, which will be adapted as soon as more information is available. Even while writing it I was able to concretise certain aspects due to more information being released.

2. Content

I firstly wish to review Wirecard's activities, and subsequently what is known about a number of potential frauds which appear to be currently emerging. In my conclusion I discuss a number of signs regarding this case that may point toward money laundering, and particularly focus on other sorts of involvement in money laundering than is currently emerging based on possible investigations in the USA and Germany.

Among other things in view of the training given by the AMLC for auditors and others, I also present a number of focal points for this target group.

For clarity's sake, this article does not aim to give an opinion on the Wirecard case, as I happily leave this to the authorities of other countries. My goal, broadly speaking, is to place the body of facts which currently appears to be emerging in a fraud and money laundering perspective, and especially to see whether we can learn anything new from the case at this stage to help us recognize large-scale organised money laundering which Wirecard may be intentionally or unintentionally involved in.

3. What sort of company is Wirecard?

Wirecard seems to have come into being, both factually and materially, around the turn of the century. It was listed on various German stock exchanges from the outset, and from 2018 on DAX[1]. Its main activity, which is important for an understanding of the relevant facts, is that it settles payments between sellers and buyers, particularly transactions concluded online. It is important to note that Wirecard is not itself in contact with these buyers and sellers. Wirecard acts as an intermediary for businesses that do have this direct relationship, such as credit card organizations. Wirecard is frequently indicated as a payment processor. What Wirecard does, is as soon as you make an online purchase with your credit/debit card or similar instruments, to ensure that the purchase is charged to the issuing bank or more specifically the bank account holding your money (your credit balance). Wirecard subsequently ensures that the money is transferred to the seller's bank account.

This is effectively therefore a very simple process, which does however require good technical facilities for fast and especially safe completion. Wirecard seems to have done this very well for many years, both technically and in terms of risks, as the company grew fast and an increasing number of reputable parties, including KLM, involved Wirecard

[1] Index with value development largest listed German companies

in their payment settlement chain. Besides Wirecard's growth due to new customers, many takeovers took place and deals were even made with big parties to carry out all their "digital" payment processes. Examples are parties such as City-bank and telecom providers.

Wirecard has branches in a large number of countries in the world, but not everywhere, and therefore has relations with third parties that also settle payments as well as having access to the countries / markets where Wirecard is not based. We are, in fact, hereby getting close to the heart of the matter where the problems appear to be. An increasing number of transactions of these third parties have taken place in countries such as Dubai, the Philippines and Singapore via 2 of Wirecard's own branches (in Ireland and Dubai). These transactions, which even amount to 60% or more of Wirecard's turnover, are now suspected of being fake. At least €.1.9 billion's worth of these transactions related to this process now seem to have disappeared from Wirecard. The amount was held via security accounts (so-called escrow accounts) for Wirecard with Philippine banks. Disappeared may even be an understatement. The money appears to have never even actually been held in the accounts.

4. Available information from open sources

After the first signs started to emerge in 2016, the situation only really gathered momentum in spring 2019, when particularly the Financial Times published information stating that it was implausible that certain third parties are jointly responsible for Wirecard's sales increases and the huge number of transactions made via Wirecard. It started with businesses in the Philippines established at the address of a marginal bus company, whose business is settled via Singapore. It was hereby indicated that the necessary information and substantiation to be expected for a listed financial company of this sort was lacking. The fact that this had been ongoing for many years was substantiated, among other things by spreadsheets and mails from 2016-2018, published by the Financial Times. After the summer of 2019 the Financial Times continued, stating that there were similar doubts regarding the extremely important Dubai partner (Al Alam), among other things seeing that Al Alam only employs 6 members of staff. This would be easy to explain if Al Alam was merely an administrative intermediary. What made it strange, however, was the fact that big credit card organisations do not seem to know this so-called third party acquirer.

Wirecard has continually directly responded to these sorts of publications by saying that the Financial Times (and other journalists) are being used by 'shortsellers' who hope to profit from a fall in the price of its shares.

In autumn 2019 the pressure on Wirecard rose so high that it asked KPMG to look into the accusations as an independent auditor. In December more publications appeared claiming the insignificance of these big customers of Wirecard. In April 2020 KPMG issued a report which was experienced very differently by Wirecard than by investors. Or as the Dutch financial newspaper FD politely indicated in the heading "Wirecard feels exonerated by KPMG report, investors remain unconvinced". It was concluded that the uncertainty around the third-party sales could not be eliminated and that the documentation necessary for substantiation was unable to be submitted. At the end of June Wirecard once again had to postpone the publication of its annual figures as the auditor (EY) was unable to issue a statement. On 23 June EY even said that "There are clear indications Wirecard was involved in a fraud with multiple parties around the world in different institutions".

The listed company subsequently went into a fast downward spiral, ultimately leading to its most important managers leaving, and a criminal investigation was instituted, among other places in Germany. The conclusion seems to be that for years, Wirecard falsely painted a too rosy picture of its books and financial statements.

These possible criminal acts are easily rightly compared to the frauds committed at Enron, Ahold and Imtech, as well as Parmalat. In essence, Wirecard appears to have influenced its financial statements, thereby misleading investors, banks and particularly social and economic life.

The financial world has been familiar with the trick used for years, and even has its own name for it: 'round-tripping'. This means falsifying high sales and the corresponding income by having the same transactions continuously running through the books. Depending on your importance as a listed company you can hereby show that you are experiencing rising market growth, which is often seen as a sign of a healthy company with good future prospects, and furthermore that you are making high profits. Pumping money around in this way and showing extra turnover is something that most businesses manage to do, but particularly accounting for this in the records and

showing where the corresponding profit has gone is more complex. Wirecard has attempted to hide the money/assets related to these transactions by claiming that the amounts concerned are held with banks in Asia.

The fraud did not, however, yet emerge as a result of targeted investigations by KPMG as materially, they merely established that the sales could not be verified, as well as errors, particularly related to Wirecard's compliance. The fraud only really emerged when the auditor EY itself asked the banks in the Philippines about the amounts held with them for Wirecard, only to hear that they had never been held there.

Alarm bells sound for the auditor

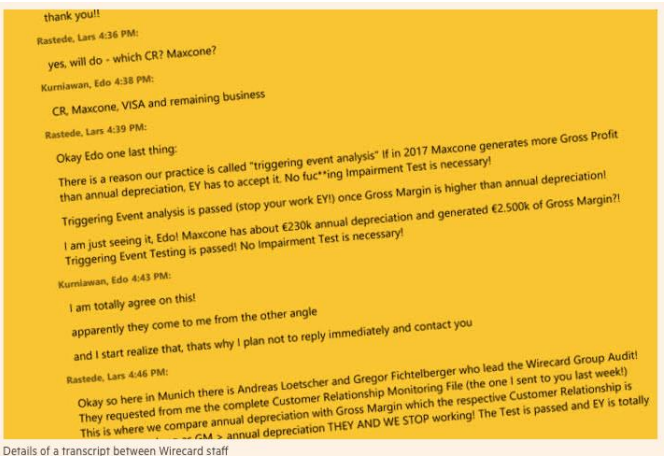
The question that many are now asking is of course self-evident: why did the auditor not request the balance as part of his auditing practice before, and conduct a critical audit regarding the existence of the amounts owed. As Marcel Pheijffer eloquently put it in the NRC: "Why choose to put such a large amount in an account far from Germany in a country where you have relatively few activities?".

Furthermore: according to the head of AMCL in the Philippines, at € 1.9 billion, the amount that should have been held was 5% of the amount in foreign currency held there. In his view, even an amount of 100 million would have been a red flag, so certainly 20 times this amount.

Even a quick glance at the financial statements and the financing structure could have prompted questions by the auditor or other interested parties. How could the company have presented a structural picture of having 3 billion in financial assets (including the 1.9 now disappeared) and at the same time have 1.75 in loans from banks? This was remarkable at the least.

In brief, I share the opinion of many that the situation should at least have indicated the necessary red flags.

But equally as important, instead of only establishing this later on, is how Wirecard allowed this to go on unnoticed all those years.


thank you!!

Rastede, Lars 4:36 PM:

yes, will do - which CR? Maxcone?

Kurniawan, Edo 4:38 PM:

CR, Maxcone, VISA and remaining business

Rastede, Lars 4:39 PM:

Okay Edo one last thing:

There is a reason our practice is called "triggering event analysis" If in 2017 Maxcone generates more Gross Profit than annual depreciation, EY has to accept it. No fuc**ing Impairment Test is necessary!

Triggering Event analysis is passed (stop your work EY!) once Gross Margin is higher than annual depreciation!

I am just seeing it, Edo! Maxcone has about €230k annual depreciation and generated €2.500k of Gross Margin?! Triggering Event Testing is passed! No Impairment Test is necessary!

Kurniawan, Edo 4:43 PM:

I am totally agree on this!

apparently they come to me from the other angle

and I start realize that, thats why I plan not to reply immediately and contact you

Rastede, Lars 4:46 PM:

Okay so here in Munich there is Andreas Loetscher and Gregor Fichtelberger who lead the Wirecard Group Audit! They requested from me the complete Customer Relationship Monitoring File (the one I sent to you last week!) This is where we compare annual depreciation with Gross Margin which the respective Customer Relationship is

Details of a transcript between Wirecard staff

Source: Financial Times, Dan McCrum 15/10/2019

In this sense it is fitting to point to the documents (spreadsheets and mails from Wirecard) I previously mentioned, which were published by the Financial Times. These clearly show that at least back in 2018 Wirecard was very consciously thinking about how the auditors their performed their audit of the financial statements. In brief, it boils down to the fact that as long as customers do not run a write-down risk everything is OK for the auditor. The wording of the internal mail from Lars Rasteder (M&A manager and as ex-staff member of an auditor's office, the point of contact for the auditor) to Edo Kurniawan (responsible for the group companies in Asia) speaks volumes: *"There is a reason our practice is called "triggering event analysis" If in 2017 Maxcone generates more Gross Profit than annual depreciation, EY has to accept it. No fuc**ing Impairment Test is necessary!"* Wirecard thus ensures that neat statements are drawn up which show that none of the big customers run a risk.

The picture presented would seem to be that the fact that this customer/these customers represent 60% of Wirecard's turnover and appear to be owed another 1.9 billion is not relevant. The situation becomes even more bizarre once you see mails dating back to 2016 indicating that the auditor had requested the substantiation of sales/income. The member of staff clearly responsible for submitting the figures regarding the sales of what would later appear to be one of the infected companies asked the above-mentioned Edo how he thought that a member of staff should draw up this statement for the auditor if he only received a statement on the sales to be booked every quarter without the underlying documents to substantiate the figures. *"How would you like to approach this topic as regards*

documenting how revenue is booked here as I only get a report usually quarterly to book revenue without the back up data to support the calculations?"

These two examples suggest that certain details were very professionally kept from the auditor, and that special care was taken to prevent the auditor from having any reason to ask more questions.

Spreadsheets published by the Financial Times, which seem to reasonably correspond with the mail correspondence, furthermore indicate other particulars regarding the booking of the sales. The commission to be received by Wirecard on what is possibly the infected transactions appears not to have been invoiced for the full 2nd quarter of 2017 for a good period after that quarter. I fully realise that billions of these third parties passed through Wirecard's books (and possibly, even through suspense accounts). But a company that fails to invoice its commission for a full quarter? This should have at least prompted questions. Or was here too care taken to ensure that the auditor did not see any underlying transactions?

Summarizing, it would strongly appear that for years, auditors received professionally orchestrated information, with the score being completely determined by the way in which the auditors had to carry out their work. On the surface, everything looked perfect and there was no reason to perform any detailed examinations In any case, the auditor does not appear to have done so.

Besides questions about how the auditor performed his work, there is more. All the usual triggers that should have been noticed when viewing the customers themselves or the market on which they are act subject to a certain distance (e.g. sales growth; type of customers; geographical structure) seem not to have been picked up. Thirdly, the usual financial and economic analyses (e.g. the relationship between bank debt and bank balance) should have also acted triggers that further examinations were required. This viewing from a distance is also an important point in recognizing possible criminal offences and money laundering.

5. The interests of the criminal

To place the information emerging in a certain perspective, we need to adopt a criminal mind-set. What could the motive to commit fraud with Wirecard's business activities? I will distinguish here between self-enrichment (whereby the loot has to be relaundered), personal status, and the money laundering of money obtained by another criminal basic offence.

5.1. Self-enrichment

Let's go back to 2004 when Markus Braun acquired power in the tiny listed company InfoGenie AG. The business at the time was a so-called penny-stock fund and the shares were therefore worth almost nothing. At the time, Braun had been CEO at (and shareholder of) Wirecard for 2 years. At the end of December, a decision was taken to have Wirecard inject capital into the virtually worthless listed company through the purchase of shares. *Effectively, Wirecard hereby very simply became a listed company*, and Wirecard's shareholders became the major shareholders. Wirecard's sales and profit then gradually increased (see the table), with the business growing on the German stock exchange until in September 2018 it was listed on the DAX.

a) Bonus as interest in fraud

On viewing Wirecard's financial statements you may notice that besides receiving a good salary, the CEO and his staff (including the COO Jan Marsalek to be discussed below) receive additional remuneration, seemingly related to the fund's performance (EBITDA).

A possible interest which could obviously be identified is that the inflation of the books was intended to benefit the financial interests of these persons in the form of salaries and bonuses.

b) Favourable takeovers as interest in fraud

Besides bonuses there are more interests, however. We see that among other things, Wirecard grew due to takeovers financed by shares. The higher the market value, the more the shares were worth, and the fewer shares had to be used to pay. The interest in acquiring valuable companies for an as low as possible price therefore benefited from a high market value, which could be achieved by inflated bookkeeping.

The question in this context is how the interested parties behind the fraud could profit from it. There are two possible indications:

1) The Hermes case:

Wirecard has had problems regarding the purchasing of the company Hermes I-Tickets Private Ltc. for years. As set out in the introduction, takeovers and purchasing companies gave Wirecard extra turnover and access to certain markets/ areas, in this case India. What is remarkable is that shortly before Hermes was purchased, Emerging Market Investment Fund (EMIF), a private equity fund established in Mauritius, suddenly entered the picture. EMIF bought Hermes for a still unknown amount, which according to the former owners was a fraction of the price of over € 300 million for which weeks later, together with another company, it was sold to Wirecard. In turn, EMIF subsequently invested another 50 million in a third business which spends considerable amounts, both directly and through affiliated other companies, on buying software from Hermes, which is now owned by Wirecard. Although this may all be very above board, it allows a considerable amount of profit to be very simply created for Wirecard by the sale of the software. However, even more conspicuous and relevant for recognizing the interests regarding the purchase and sale of Hermes is the fact that there are also strong indications that the COO of Wirecard (Marsalek) is affiliated with EMIF, which has made a considerable profit.

> *Sham litigation as legitimacy and cover up?*
>
> *Furthermore, various legal proceedings are taking place around this case. An English judge recently indicated that he did not require additional documents, seeing as the case of the former owners against Wirecard could effectively settled without further handling. This could, of course, concern an ordinary (civil) case. However, conducting "sham litigations" as a means of legitimizing transactions is a well-known trick in the money laundering world.*[2]

2) Payment for "3D secure tokenisation" software:

Let's go back to profiting from purchases and the wrongful withdrawal of money from a company. In 2019 the Financial Times wrote that the Indian branch of Wirecard had once again bought 3 million worth of "3D secure tokenisation" software. Among others, the payments were once again made through Hermes. However, the seller did not know the buyer and was not familiar with the sold product. Even more to the point, no business was done in India. In brief, expenditure of 3 million for no reason. The question is, what has happened to the money. Who benefitted from Wirecard spending 3 million? Furthermore, the financial handling appeared to have taken place through Wirecard's own channels.

I would like to summarize these variants as modus operandi effectively involving the "theft" of money of Wirecard by overpaying or paying for non-existent products. It is abundantly clear that intentionally created concealment constructions and falsity are made use of. It is also self-evident that via a concealment construction, the money obtained then flowed back to the frauds, possibly including Wirecard's directors. If proof is found of this, it is highly likely that this would be typified in the Netherlands as money laundering in its purest form.

c) Overvalued shares as interest for fraud

Another very obvious reason to drive up the price as much as possible is to profit from the sale of the shares to guileless investors. As set out above, Wirecard became a listed company by making a contribution to the penny-

[2] Listen to the podcast 'Witwassen in het nieuws' [Money laundering in the news], at https://www.amlc.nl/podcasts/

stock fund, upon which Wirecard's owners obtained the shares. The fact that the CEO was one of the major shareholders is clear if you are aware, as I discuss later on, that shortly before the big clash he sold a huge interest in shares in the company.

Many more instances of self-enrichment can be mentioned, but regarding the step to money laundering, the foregoing are exemplary.

5.2. Social pressure and personal status

As mentioned above, I do not rule out that the interests set out above were an important reason for the action taken.

However, we must not close our eyes to the possibility that external pressure (investors) for good results and to show market growth were important motives. As set out above, this could be achieved by taking over and of course the full consolidation of the companies purchased. Payment by the overvalued shares was thereby a perfect instrument.

Many of the CEOs et al. of the businesses involved in these sorts of frauds have been under social pressure. Or as one of them put it a few years ago during a lecture for auditors and students at the University of Maastricht: "After I had been working for the listed company for 3 months, I called my former colleagues to tell them: we thought we knew how to influence figures, but that was nothing compared to what they do here in this company!". In response to the question from the audience why he was not stopped and whether no one had warned him that he was playing a dangerous game, he answered: "I had to get results for my shareholders and the analysts, and in MY environment, you didn't answer back. I was the entrepreneur of the year!" CEO Markus Braun and his staff were possibly in the same position.

> *Speculating with shares in your own company as collateral.*
> *Speaking of egos and financial interests, another brief comment I promised, which may give an impression of the interests involved.*
> *It is especially noticeable that according to publications, when the price began to fall dramatically in response to publications regarding possible fraud, Braun had to sell a large part of his shares in Wirecard. He had to increase the margin commitment by € 150 million. He had taken positions using borrowed money, as a result of which in the falling market at the time, with this sale, there was an extra offer.*
>
> *The fact that Braun was not the only one to use this construction of borrowing money with shares in your own company is evident if we look back a few months. We see that in April, Goldman Sachs also forced the Chinese billionaire Lu Zhengyao to sell a large part of his share package, again to comply with a margin commitment.*
> *An example of how a private investment can have big consequences, not just for the private person, but also for the business, as soon as heavy weather is run into.*

5.3. The 'high end' money laundering construction

Until now I have focused on the private interests that may be behind the possible bookkeeping fraud, regarding both financial and ego/social pressure. But other interests may also play a role. This brings us to a potential high end money laundering construction.

In connection with criminal investigations, the Americans are examining Wirecard's involvement in a drugs market place, whereby third-party payment processors were used to settle credit card payments for drugs. They have suggested that Wirecard played a role, in various positions, in this payment settlement chain for these purchases. Furthermore, apparently in 2015 too, Wirecard received a "visit" from the Public Prosecution Service in connection with a money laundering investigation in the US, and in 2010 an investigation mentioning Wirecard was conducted into a German who handled transactions related to gambling in online casinos in the US, without a licence.

The fact that Wirecard has handled payments in situations in which an American gambled or bought drugs via his bank or credit card is also unremarkable; this is precisely their business model.

We must not stop here; more important is, as many suggest, that we examine Wirecard's active involvement and the fact that Wirecard is aware that it transfers money related to criminal offences or obtained through criminal offences (and had a role in a money laundering procedure). The high end money laundering construction is further examined in the next chapter.

6. Wirecard as money laundering machine

6.1. Possibilities for a business model

It can be established that Wirecard's business model has a number of elements that could make it attractive to money launderers:

- Wirecard's primary activities are in the area of transferring money based on third parties' buying and selling transactions. Wirecard is thereby actually never the bank or payment organisation directly related to the buyer and seller; any transactions with a money laundering goal will not be easily picked up, given that there is no direct insight into actual purchases and sales.
- International money flows exist which on one hand comply with interests in transferring money from one country to another, and on the other hand make money flows more difficult to monitor.
- Wirecard is furthermore a company which handles a great number of transactions and therefore, transactions which are only intended to facilitate money laundering can easily hide among the huge numbers.
- Lastly, Wirecard's status as a listed company gives it an impression of reliability. Whoever would suspect a listed company, with all the concomitant auditing, of being involved in money laundering?

This makes Wirecard an ideal instrument for money launderers to have play a role in their money laundering constructions. But how can Wirecard be involved in this? And must Wirecard have always been actively involved and have known what was going on, or might Wirecard have been unintentionally used in money laundering constructions?

6.2. Money laundering goals

By using Wirecard in a money laundering construction, a money launderer:

1) could show a large 'legitimate' profit by making profit on (fake) trade transactions (legitimated) (6.2.1.)
2) could use trade transactions to circumvent restrictions meaning that he cannot access his black money in or from a certain country or convert it into another currency; examples are foreign exchange restrictions, strict anti-money laundering rules/ gatewatchers or sanction measures (placing, transferring, concealing) (6.2.2.)

I will show that these money laundering goals are not only able to be achieved by using Wirecard's trade transactions, but also by using the listed company itself as a money laundering instrument (6.2.3.).

6.2.1. Creating profit via fake sales

In variant 1) the money laundering organization can relatively easily create a big money circulation, whereby money from criminal parties is converted into trade transactions and the profits benefit the seller or the service provider. Behind the seller are the criminal organisations who make legitimate profit in this way. What might this look like in practice?

As the seller, a company is chosen which has a strong relationship between sales and any goods. Examples are gambling sites, porn or chat services, or call centres people call to for large amounts. Ordinary internet deliveries are also suitable. The money launderer sets up an automated service (e.g. calling the call centre or buying from the internet seller). The payment is handled via a payment processor such as Wirecard. The new company is a booming business and makes a lot of profit. As part of the procedure, before the money arrives at the payment processor's, it is introduced into the system with a great number of other legal transactions. Because this takes place via various links, some of which are often intransparent, it is virtually impossible to see where the money from the criminal organization came from.

The contribution may naturally also take place transparently. A good money launderer, however, will make sure that the audit trail of the money flows is impeded in another way. Examples of other ways are not just the use of new means of payment such as Bitcoins, Monero etc. but also pre-paid pay-cards or simply pre-paid telephone cards (credit balances).

If we now look at what is known about Wirecard we see that insofar as transactions can be traced, a very large part go to companies like gambling or porn businesses, etc. Of the businesses that can somewhat be traced it remains fairly unclear how they can be doing so well. The fact that given the services it provides Wirecard carries out a lot of work for businesses which provide these kinds of services via the Internet is not in itself remarkable. However, the huge scope of the transactions and the extremely strong growth of their scope IS remarkable. However, the way in which money flows take place via obscure businesses in less transparent countries and partly the obscure and concealed structures that are used give us, the Public Prosecution Service, at the least a reason to further examine these transactions. The question of whether Wirecard is intentionally or unintentionally involved then certainly arises. However, given the scope and the active role played by the management in concealing the nature of the figures, I am starting to have the necessary doubts about whether Wirecard was not very intentionally set up to enable these sorts of transactions without lots of questions being involved.

> *The advantages and drawbacks of selling goods compared to services in connection with a money laundering transaction*
>
> *During trainings I am often asked whether using goods-related internet sales is not a risk, and if as a money launderer, you should particularly avoid using them. It is basically correct that services like gambling, porn, call-centres etc. carry less risk. However, it is also true that these branches are more inclined to be seen as being high-risk. Consequently, money launderers do not like to make use of high-risk branches. Even more so, money launderers want to prevent auditors from refraining from issuing an opinion in connection with financial statements (because the opinion provides precisely what the money launderer wants, namely a semblance of legitimacy). This is solely because an auditor's office does not want any customers from these branches. This is the reason why ordinary internet trade is very suitable. Money launderers just have to make sure that the buyer and seller are both aware that nothing will ever actually be delivered, and the only goal is the seller's profit. This means that if the buyer and seller are part of the same criminal organisation there will never be any complaints, and the seller's flow of fake purchase invoices for the sales and the sending of empty boxes is more than sufficient proof.*[3]

6.2.2. Transferring money or converting currencies via fake sales

This modus operandi can be used for the 2nd interest in virtually the same manner. Because related to the fake sales or services, money also needs to be transferred. Especially if a big payment processor is part of the chain, listed on the stock exchange and from a country known for its "gründlichkeit", the risk of questions being asked is very small. The big advantage in this regard is that a payment amount is concerned and not the profit made on it.

In brief, if you are able, as a criminal organisation, to set up a business in such a crucial spot in the financial chain as Wirecard as payment processor, and you are also able to have it listed on the stock exchange and to end up with a listing on the biggest stock exchange of a trustworthy country like Germany, you will have a great instrument at your disposal to organize the money flows you require in connection with money laundering. You would naturally want to make use of this service. A good money launderer will always have criminal activities incorporated into legitimate business, as this is the way to fly under the radar. In actual case, questions about Wirecard's activities and the scope of its activities have been asked for years, but with the exception of a couple of journalists we all missed it.

6.3.3. Employing the listed company's own activities as a money laundering instrument

I wish to continue, however. If, after all, you have the listed company in your possession, a money launderer can use it as a highly reliable instrument. A listed company purchasing participations and making large investments

[3] Listen to the podcast 'Business typologies' [Bedrijfstypologieen], at https://www.amlc.nl/podcasts/

and consequently large payments will be sure not to raise any eyebrows. Even more to the point, everyone knows that these sorts of activities often concern large amounts. So why, as a criminal, instead of going to a lot of work setting up a system of fake transactions, even involving sending empty boxes as described under 1) and 2), would I not have myself paid now and again for the sale of a new participation which will serve to grow the listed company? The fact that the company is a good investment and will generate turnover is clear, given that I will subsequently simply allow the transactions I need under 1) and 2) to take place as otherwise. It would be a good idea to further examine whether the purchases made by Wirecard are also related to the above. The 2 previously mentioned deals regarding India suggest that Wirecard may not be an blank page in this regard.

If this variant has been used, there can effectively be no doubt that at least the top of Wirecard has been involved in influencing figures as well as money laundering or other criminal offences. This will have to be substantiated by the facts.

> *Speculation in your own listed company as money laundering instrument*
>
> *I wish to make another short remark in connection with this variant. A listed company is particularly useful to allow legitimate profit to flow to the investors in these companies. If there was ever a fund subject to price fluctuations it was Wirecard these past years. Wirecard has continually professionally responded that its price fluctuations are caused by outsiders. This is designed to prevent anyone from looking at the company itself. But if you look back and see, among other things, that CEO Braun was apparently known to have a very large margin commitment and that there were also announcements that despite the restrictions applicable to him he realised by sales on at least the 3 days before the problems begun, we must ask who the other parties were who profited from the price fluctuations in the past. Here too, it's possible that on the surface, everything was done by the (formal) rules. But if you see the indications here that a listed company was clearly used, possibly for money laundering purposes, it is definitely worth the trouble of also looking into this option.*

7. Conclusion

This goal of this article is not to make any claims about Wirecard or persons possibly involved in this case. My goal, as requested by many people, was to project a number of the options for fraud and money laundering onto the Wirecard case. I tried to do this as far as possible based on the information that has emerged. Whether or not the information is all correct will have to be established later on. I did not necessarily attempt to provide a comprehensive account. As in our training 'Edje van Utrecht' I aim to encourage people to further activate their minds; if this can be done, so can that. Whether the possibilities I have mentioned actually took place, as was the case with the article about money laundering involving games from a number of years ago, remains to be seen. I have noticed that during the last 2 weeks, some of the options I included in my initial set-up have been substantiated by publications.

It is precisely for this reason that I have opted for an open-end article, which I will definitely adapt if more information emerges. I have limited myself to matters that are actually relevant for combatting money laundering and for gatewatchers such as auditors. I have omitted mentioning the fact that there is much more to say regarding the disappearing COO, which may be related to secret services, and the fact that a well-known hackers group has suddenly become very active around Wirecard's downfall.

If after reading this article you have any questions, see new signs or wish to look into certain aspects in more depth, feel free to contact AMLC where we are working on combatting money laundering together.

I will finish by expressing the wish that we learn 'to look differently' for the fight against high-end money laundering. More based on hypotheses about what money launderers will do based on their interests, and how they make use of situations that we see as normal or even trustworthy. I hope that this article will be an impetus to this end. I am, in any case, going to take another good look at particulars regarding listed companies, because Wirecard has given us lots of extra red flags which to a certain extent should have been recognized in connection with earlier frauds.

Case law

Amsterdam Court of Appeal, 23 June 2020, disciplinary action against civil-law notary for non-compliance with obligations under Money Laundering and Terrorism Financing (Prevention) Act (WWFT): ECLI:NL:GHAMS:2020:1550

The Financial Supervision Office (in Dutch: BFT) has determined that a civil-law notary failed to meet the obligations under the Money Laundering and Terrorism Financing (Prevention) Act (in Dutch: WWFT) because he/she did not carry out an intensive client investigation, did not satisfy the obligation to monitor, and showed negligence in reporting unusual transactions to the FIU. For these reasons, BFT submitted a disciplinary complaint to the national civil-law notary and court bailiff's association of the Netherlands. The association declared the complaints about failing to carry out an intensive client investigation and not satisfying the obligation to monitor inadmissible. BFT launched an appeal against this decision because it was of the opinion that the association had erroneously held that the BFT was not allowed to submit disciplinary complaints against civil-law notaries for transgressing the WWFT. The Court of Appeal agrees with the BFT that, in general, a violation of the WWFT falls under the disciplinary standards of Article 93 of the Notaries Act (in Dutch: WNA). Every time a civil-law notary offers his/her services, the actions undertaken are supplemented by obligations under the WWFT. This is inherent in the gatekeeper's role that civil-law notaries have been assigned by Dutch legislators. Therefore, fulfilling obligations under the WWFT cannot be seen as separate from committing or omitting to act properly in the eyes of the law. The Court of Appeal thus found that compliance with the obligations of the WWFT is so closely bound up with the actions or negligence of a civil-law notary, that the civil-law notary can be charged with non-compliance with WWFT obligations on the grounds of disciplinary rules governing civil-law notaries.

Therefore, the Financial Supervision Office (BFT) is entitled to submit a disciplinary complaint against a civil-law notary for violating WWFT obligations.

District Court of Amsterdam, Court in Interlocutory Proceedings, 3 July 2020, a bank is not obliged, for the time being, to return account balances to fraudulent account holders due to the risk of money laundering, ECLI:NL:RBAMS:2020:3283

ING Bank has blocked two commercial accounts of clients because the bank has received information that money deriving from invoice fraud has been parked in these accounts. The bank had already reported this fraud, and the client relationship had already been terminated.

The termination of the client relationship has not been contested, but ING Bank retaining the account balances (approximately 220,000 euros) has been challenged, since as a consequence of this action the account holders' commercial operations have come under threat. ING argued that it cannot proceed to pay out the amounts because it is forbidden to on the grounds of anti-money laundering laws, and it would risk a criminal prosecution for debt money laundering, as well as liability claims from third parties in connection with its special duty of care; there is also an issue of reputational risk. An investigation into the origins of the funds is still on-going.

The judge in interlocutory proceedings found: 'If ING proceeds to pay out the account balances, it cannot be ruled out that it would thereby be guilty of violating Article 5(1) of the WWFT or (complicit) in debt money laundering or some other criminal act'. For the time being, ING is not required to pay back the remaining balances.
On the grounds of Article 5(1) of the WWFT, a bank is prohibited from conducting transactions for a client as long as the client investigation cannot be successfully completed.

Colofon

mr. Dorine Stahlie
mr. Sophie de Ridder
mr. Ruut Regtering

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

E: AML.Centre_Postbus@belastingdienst.nl

To subscribe or unsubscribe, please send an email

ANTI MONEY
LAUNDERING
CENTRE