ECLI:NL:RBOBR:2024:2069

Authority	East Brabant District Court
Date of decision	14-05-2024
Date of publication	14-05-2024
Case number	82/198261-22
Areas of law	Criminal law
Special features	First instance - plural
Content indication	Conviction for laundering large amounts of crypto currency. Together with his co-perpetrators, the defendant developed Tornado Cash. Tornado Cash was developed so that it automatically performs the actions essential for money laundering. Tornado Cash combines maximum anonymity and optimal concealment techniques on the one hand, with a severe lack of functionalities enabling identification, verification or detection on the other. As a result, Tornado Cash cannot be characterised as a legitimate tool unintentionally misused by criminals. With blinders on, completely ignoring the abuse that took place through and by Tornado Cash, the defendant continued to develop and exploit Tornado Cash. The court imposed a sentence of 64 months' imprisonment.
Findings	Rechtspraak.nl

Excerpt

—

judgment

COURT IN EAST-BRABANT

Location 's-Hertogenbosch

Criminal law

Prosecution number: 82.198261.22.

Date of judgment: 14 May 2024.

Judgment of the East Brabant District Court, Plenary Criminal Chamber, in the case against:

[defendant] ,

born [1993] , living at

[residential address] .

This judgment was rendered in rebuttal following the hearing of 22 November 2022, 15 February 2023, 20 April 2023, 24 May 2023, 13 September 2023, 26 and 27 March 2024
and 30 April 2024.

The court took note of the prosecution's claim and what was put forward by the accused.

1 The indictment.

The case was brought by summons dated 27 September 2022. After the indictment was amended at the hearing on 26 March 2024, the accused was charged with:

he, at one or more times in the period from 9 July 2019 to 10 August 2022 inclusive, in Amstelveen, or at least in the Netherlands and/or in Russia and/or in the United States and/or in Dubai, together and in association, or at least alone, made a habit of committing money laundering, or at least laundered,
After all, the defendant and/or his co-perpetrator(s) have/have been in possession of (an) object(s), namely (approximately) 535,809 crypto currency (ETH) (worth (approximately) $1,217,343,820) (Money Laundering Case File page 108/109 jo DOC-33a , page 3263 et seq.), consisting of
- 50,930 ETH (sourced from [internet site 1])
- 7,466 ETH (sourced from [internet site 2])
- 14,012 ETH (sourced from [internet site 3])
- 2,420 ETH (sourced from [internet site 4])
- 2,994 ETH (sourced from [internet site 5])
- 6,628 ETH (sourced from [internet site 6])
- 2,410 (taken from [internet site 7])
- 7,204 ETH (sourced from [internet site 8])
- 2,037 ETH (sourced from [internet site 9])
- 4,004 ETH (sourced from [internet site 10])
- 5,855 ETH (sourced from [Internet site 11])
- 8,264 ETH (sourced from [internet site 12])
- 2,026 ETH (sourced from [Internet site 13])
- 17,181 ETH (sourced from [internet site 14])
- 3,223 ETH (sourced from [internet site 15])
- 2,023 ETH (sourced from [internetsite 16])
- 4,900 ETH (sourced from [internet site 17])
- 9,300 ETH (sourced from [internet site 18])
- 2,200 ETH (sourced from [internet site 19])
- 30,397 ETH (sourced from [internet site 20])
- 2,560 ETH (sourced from [internet site 21])
- 1,971 ETH (sourced from [internet site 22])
- 7,500 ETH (sourced from [internet site 23])
- 2,794 ETH (sourced from [internet site 24])
- 10,290 ETH (sourced from [internet site 25])
- 2363 ETH (taken from [Internet site 26])
- 2,116 EHT (taken from [internet site 27])
- 8,801 ETH (sourced from [internet site 28])
- 4,566 ETH (sourced from [internet site 29])
- 175,100 ETH (sourced from [internet site 30])

- 24,849 ETH (sourced from [Internet site 31])
- 5,446 ETH (sourced from [internet site 32])
- 3,931 ETH (sourced from [internet site 33])
- 85,700 ETH (sourced from [internet site 34])
- 7,561 ETH (sourced from [internet site 35])
- 4,787 ETH (sourced from [internet site 36])
concealed or disguised the origin and/or movement and/or concealed or disguised who the rightful owner(s) of the object(s) was/were and/or concealed or disguised who held the object(s),

while the accused and/or his co-perpetrator(s) (in each case) knew, or at least reasonably should have suspected, that the object(s) in whole or in part - immediately or indirectly - originated from any crime.

Insofar as the indictment contains linguistic and/or writing errors, these have been corrected in the statement of facts. As appears from the proceedings at the court hearing, the accused's defence has not been impaired as a result.

2 Introduction.

On 21 July 2022, the criminal investigation into the operation and use of [crypto system] . The investigation was named Kidwelly. The reason for the investigation was that various news reports and reports revealed that [crypto-system] was allegedly used to disguise cash flows originating from digital thefts (hereinafter: hacks).

The criminal investigation looked into possible people involved in [crypto-system] . By studying the GitHub page of [crypto-system], suspicion arose that the accused was one of the developers of [crypto-system]. The criminal investigation then also focused on the defendant.

Defendant is charged with co-perpetration of habitual money laundering following the Kidwelly investigation.

3 The formal preliminary questions.

3.1 The validity of the subpoena.

Defence position.

The defence argued that the summons should be annulled because the indictment did not meet the requirement of certainty under Section 261 of the Code of Criminal Procedure (hereafter Sv). The defence argues that the indictment is insufficiently specific. The term [crypto system] is not even included in the indictment, while [crypto system] plays a crucial role in the charge. The indictment does not describe on what manner the money laundering is alleged to have taken place via [crypto system], which hampered the defence from responding adequately to the allegation and preparing the case.

Prosecutor's position.

The prosecutor argued that the summons met the requirements of section 261 Sv and that the proceedings at the hearing showed that the defence also knew what the charge was about.

The court's verdict.

Article 261 Sv contains some minimum requirements for the indictment. When interpreting Article 261 Sv, the key question is whether the accused can properly defend himself on the basis of the indictment. In the court's opinion, the indictment meets these requirements. Viewed in conjunction with the criminal file, the indictment contains a sufficiently specific indication of the charge. The court notes that during the court hearing it also appeared in fact that the charge was clear to the defence. The court rejects the defence pleading that the summons is null and void.

The court notes that the examination at the hearing showed that the summons was valid and that it complied with all legal requirements.

3.2 **The admissibility of the prosecution.**

Defence position.

The defence argues that the prosecution considers the accused to be a digital online service provider and that if the court follows this position, the prosecution should be declared inadmissible on the basis of article 54a of the Criminal Code (Sr). To this end, the defence argues that article 54a Sr excludes the prosecution of internet intermediaries when an order given to them by the public prosecutor under article 125p Sv is complied with. This power to order implies in principle that the public prosecutor is obliged to issue such an order prior to a prosecution, failing which the public prosecutor is inadmissible in the prosecution. As the public prosecutor did not issue an order to the accused under section 125p Sv, the public prosecutor should be declared inadmissible under section 54a Sr.

Prosecutor's position.

The public prosecutor argued that section 54a Sr did not apply because the accused was not an intermediary providing a telecommunication service as referred to in section 54a Sr.

The court's verdict.

The legal regulation.

Article 54a Sr read as follows from 1 March 2019 to 1 September 2023:

An intermediary who provides a communication service consisting in the transmission or storage of data originating from another person shall not be prosecuted as such in the case of an offence committed using that service if he complies with an order referred to in Article 125p of the Code of Criminal Procedure.

Article 125p(1) Sv reads as follows:

In case of suspicion of an offence as described in section 67(1), the public prosecutor may address to a communications service provider as referred to in section 138g the order *to immediately take all measures reasonably required of it to render inaccessible certain data stored or transmitted, insofar as this is necessary to terminate a criminal offence or to prevent new criminal offences.*

Article 138g Sv reads as follows:

Provider of a communication service means the natural or legal person who, in the course of a profession or business, enables users of his service to communicate by means of an automated work, or processes or stores data for the purpose of such a service or the users of that service.

It follows from the legislative history that this regulation is specifically intended to support freedom of expression. An intermediary providing a communication service is immune from criminal liability if it makes inaccessible criminal data transmitted or stored by means of the communication service as soon as the public prosecutor issues an order to that effect. As a result, the intermediary need not feel compelled to engage in preventive censorship (House of Representatives, session year 2001-2002, 28197, no. 3, p. 63).

The review.

The defendant has developed software that allows cryptocurrencies to be moved anonymously and has made this software available to users online. In the court's opinion, it is thus evident that the accused cannot be regarded as a person who, in the exercise of a profession or business, offers the users of his service the opportunity to communicate by means of an automated work, or processes or stores data for the benefit of such a service or the users of that service within the meaning of Section 138g Sv. An order within the meaning of Section 125p(1) of the Code of Criminal Procedure cannot therefore be issued to the accused. Moreover, it is also impossible to see which data should be made inaccessible by the accused. Following on from this, the court is of the opinion that the accused cannot be regarded as an intermediary as referred to in article 54a of the Criminal Code either. The prosecution exclusion ground therefore does not apply to the defendant.

Conclusion.

The court rejects the defence's defence of inadmissibility. The investigation at the hearing did not reveal any other circumstances preventing the prosecution from being admissible. The Public Prosecution Service can be received in the prosecution of the accused.

3.3 The remaining preliminary questions.

The court has jurisdiction over the charges. Furthermore, no grounds for suspension of the prosecution have emerged.

4 The evidence and its assessment.

The evidence.

For the sake of readability of the judgment, reference is made to the elaboration of the evidence used by the court. This elaboration is attached as an appendix to this judgment and the contents of that appendix should be considered repeated and inserted here. The court bases its judgment on the evidence contained in this evidence annex. Due to readability and verifiability, the court has also included footnotes in its considerations.

Prosecutor's position.

The public prosecutor considers legally and convincingly proven that the accused, together with others, were guilty of habitual money laundering. By developing, offering and improving the service [crypto-system], they concealed or disguised where the crime-derived Ether mentioned in the indictment went, where it came from and who owned the Ether at the time of deposit and the time of withdrawal.

Defence position.

The defence pleaded acquittal, arguing inter alia the following. The defendant had no intent in the conduct charged. The intention of the developers of [crypto-system] was never to break the law or facilitate criminal activity, but was to provide a legitimate privacy solution to a growing need in the crypto community. As such, [crypto-system] is a privacy tool that seeks to meet a legitimate need. It is up to the user not to misuse this software for illegal purposes. The facts and circumstances show that the accused did not accept this misuse of [crypto-system]. The technical features of [crypto-system] make effective action against the misuse impossible.

The court's verdict.

In order to answer the question whether the accused was guilty of the charges, the court must assess whether all the components of the indictment were fulfilled. The court will discuss those constituents below.

- *Object within the meaning of Article 420bis Sr.*

The object of money laundering in this case is 535,809 ETH (Ether), worth about USD 1,217,343,820 (US dollars).1

There have been several judgments and rulings in case law ruling that Bitcoins are objects that can be laundered.2 The public prosecutor equates Ether with Bitcoins. According to counsel, the Supreme Court has not yet explicitly ruled on whether Bitcoins are objects within the meaning of Article 420bis of the Criminal Code.

The court ignores the defence's comment and follows previous rulings on Bitcoins. Like Bitcoins, Ether are crypto-currencies, digital money units, which represent a real economic value, are susceptible to human control and are

are transferable. Therefore, the court finds that the Ether charged are objects within the meaning of Article 420bis of the Criminal Code.

- Derived from any crime.

The object being laundered must originate from a prior crime (predicate offence). There is no need to charge and prove by whom, when and where that crime was committed. The defence has argued that with regard to the Ether listed in the indictment, there are no concrete predicate offences, so that it would have to be assessed using the six-step plan laid down in case law whether the Ether originated from any crime.

Based on the evidence, the court finds that the charged Ether originated from 36 separate hacks.3 It follows that the charged Ether originated from theft with a false key (section 311 of the Criminal Code), whether or not in conjunction with other crimes. The charged Ether thus originate from specifically identifiable crimes. The six-step plan is therefore not at issue.

- Hiding and concealing.

The assessment framework.

Money laundering is often described in the literature as a process in which three phases can be distinguished. It involves placing criminal assets in the financial system, disguising the criminal assets making them difficult to trace, and integrating criminal assets by giving them a seemingly legal origin allowing them to be used without the criminal origin being visible. In the case of suspected money laundering, it is not required that all stages of money laundering have been completed. Conduct occurring within one or more of these stages may in itself constitute a criminal offence.4

This case involves the money laundering acts of concealment and disguise from Article 420bis paragraph 1 under a of the Criminal Code. These acts are aimed at making it difficult to see the origin of objects, the movement of objects and who the rightful owners of the objects are.

The law does not specify which acts may be involved. The legislative history shows that the effect of the act determines criminality. Thus, the terms conceal and disguise imply a certain purposefulness. The act is aimed at making it more difficult to see the nature, origin, location, etc. of objects and is also suitable for achieving that purpose. There need not be any question of making the true nature, origin, location etc. completely invisible. Concealment and disguise will already be possible if certain constructions create a curtain of mist that, while allowing some view of the object and the persons involved, do not make it possible to establish with any certainty the (legal) provenance and the rightful owner.5

The legislative history further shows that it is not required that a suspect has the object of money laundering in his possession or control. A distinction must be made between the act described in subsection a of the first paragraph of Articles 420a and the acts described in subsection b. The latter acts (acquisition, possession, transfer, conversion or

make use of an object derived from crime) presuppose some actual control over the object. This is different in the case of concealment and disguise referred to in subsection a.
Under circumstances, a person may be guilty of this who does not actually have the object in question in his possession or control. This is already clear from the fact that this includes a person who conceals or disguises who is the rightful owner of an object or has it in his possession. In that case, it is not the accused but someone else who has the object in his possession in a legal or factual sense.6

The operation of [crypto system] .

The prosecution argues that there is concealment and disguise by (the [crypto-system] developed and launched online by the accused) . Therefore, it is important to first look at how [crypto-system] .

[crypto-system] will be introduced to the market in August 2019 with an article explaining what [crypto-system] can do. That article proclaimed that [crypto-system] enables users to conduct 100% anonymous transactions with crypto-currencies on the Ethereum blockchain.7 It was with that goal of ensuring privacy in financial transactions that [crypto-system] was developed.8

[crypto-system] has been operational on the Ethereum blockchain since 2 August 2019. Although [crypto system] has undergone several developments since then (more on this later), the operation of [crypto system] essentially boils down to the following.9

[crypto system] employs so-called pools, a kind of collection buckets, which accept deposits of crypto currency from one wallet address and allow withdrawals via another wallet address. This breaks the link between a deposit and a withdrawal.

Each pool has its own smart contract. These smart contracts are placed on the Ethereum blockchain. Because of the way the blockchain works, it is technically impossible to take these smart contracts offline. Smart contracts are so-called autonomous functionalities. They are codes programmed to automatically execute a command when a certain condition occurs.10

[crypto system] has multiple pools. In the case of the cryptocurrency Ether, these are pools in the size of 0.1, 1, 10 or 100 Ether. This means that only Ether in those individual pools can be deposited and withdrawn in those respective quantities. The use of uniform quantities increases user anonymity. In this way, deposits and withdrawals cannot still be linked based on the size of the amounts themselves.

The simplest way to access [crypto system] is through the user interface (hereinafter: UI), or online user environment. To host the UI, the Inter Planetory File System (hereinafter: IPFS) has been used since May 2020. IPFS is a decentralised distributed file system that allows files to be made available without having to be stored in a central location. Due to the nature of how this system works, it is as good as impossible to make the user interface inaccessible. This fact, combined with the use of smart contracts, makes it practically impossible to take [crypto system] offline.11

The use of [crypto system] is completely anonymous. Both when depositing and withdrawing cryptocurrencies, no identifying information needs to be provided. Also, no Know Your Transaction (hereinafter KYT) verification takes place (more on this later).12

[crypto system] uses zk-SNARK technology. Through that technology, users can prove possession of information without having to reveal that information.

[crypto-system] is a decentralised non-custodial protocol, which means that the user of [crypto-system] remains in full control of the cryptocurrency they deposit. At no time does [crypto-system] obtain power of disposition or control over the deposited cryptocurrency.

Management of the deposited cryptocurrency takes place via the deposit receipt. The user who makes a deposit receives a proof of this deposit, called a note. The possessor of the note can use that note to withdraw the deposited cryptocurrency. Without a note, making a withdrawal is not possible.

The user of [crypto system], when making a withdrawal from [crypto system], has the choice of making that withdrawal himself, via his own chosen wallet address, or having that withdrawal made by a so-called relayer.

Relayers are externally managed systems, servers, that execute a transaction on behalf of a user after being instructed to do so. Without a relayer, a user would leave a traceable trail on the blockchain that could reveal his identity. Indeed, for every transaction a user makes, they must pay a fee (fee) to [crypto system]. That fee can be traced back to its payer, via the wallet address he uses for that purpose.

A user does not run that risk if he uses a relayer to withdraw the cryptocurrency. The relayer acts as an intermediary and arranges the entire withdrawal, including payment of the fee. The relayer pays the fee by deducting it directly from the amount withdrawn. The fee is thus no longer traceable to the person receiving the cryptocurrency. The relayer system therefore further safeguards user privacy. The relayer provides an additional layer of anonymity.13

It thus follows from the above that [crypto-system] is able to break the transaction trail on the Ethereum blockchain for a user who remains completely anonymous. This is done by [crypto-system] by cutting the link between the delivering wallet address and the destination address on the blockchain. As a result, the transaction trace of the crypto-currency in question stops at [crypto system] .

Executive role of [crypto system] .

The defence has put forward that only the user of [crypto system], by abusing [crypto system] , is guilty of money laundering. In this regard, the court notes the following.

The court noted above that it is [crypto-system] that breaks the link between a deposit and a withdrawal. By breaking that link between a deposit and a withdrawal, [crypto-system] conceals or hides what the original origin of the withdrawn cryptocurrency is, who the actual owner is and where the cryptocurrency is moved to. By allowing [crypto-system] to make completely anonymous deposits into and withdrawals from [crypto-system], [crypto-system] also conceals or disguises who has the actual power of disposal of the crypto-currency, that is, who holds the crypto-currency.

When these acts are performed in respect of crime-derived Ether, it is actually [crypto system] that gives effect to the concealment or concealment money laundering act.
Therefore, in the court's opinion, [crypto system] cannot be seen as merely a tool for the user.

The fact that [crypto system], in carrying out these concealing or disguising money laundering acts, at no time had power of disposal over the cryptocurrency derived from crime does not alter this. After all, there is no requirement to have power of disposal over the laundered objects in order to carry out these acts of money laundering.

Neither does the fact that possibly the user may also be guilty of money laundering in respect of the same cryptocurrency, for example in the form of transferring, moving or possessing the criminally derived cryptocurrency. Different persons and/or instruments may be guilty of laundering the same proceeds of crime in different ways.

Conclusion.

The court concludes that [crypto system] carried out money laundering acts, namely concealing or hiding the origin and movement of felony-derived cryptocurrency, Ether, who were its rightholders and who actually (had) possession of it.

- Is defendant responsible for the execution by [crypto system] ?

The defence has argued that the defendant had no (more) influence on the autonomously operating smart contracts of [crypto system] . The defence thereby places the accused as an unwilling and impotent third party at a distance from the unstoppable money laundering acts of [crypto-system] . Insofar as the defence thereby meant to say that the defendant cannot be held responsible for those money laundering acts carried out by [crypto-system], the court considers the following.

A page has been created on GitHub for [crypto system] . GitHub is an online platform for software development and version control. An analysis of [crypto-system]'s GitHub page shows

That the defendant is one of the three users who made the most contributions to the source codes of [crypto system] . The other two users are [co-defendant 1] (hereinafter: [co-defendant 1]) and [co-defendant 2] (hereinafter: [co-defendant 2]).14

In his own words, the defendant developed the source codes for the pools, the UI and the relayer software of [crypto system]. The defendant did this together with the team.15 In the court's opinion, this unmistakably refers to the defendant, [co-defendant 1] and [co-defendant 2] .

The court regards the defendant, [co-defendant 1] and [co-defendant 2] as the founders of [crypto-system] . Besides the fact that they developed the core functions of [crypto-system], it follows from the case file that they behaved as the management of [crypto-system] and also presented themselves as such to third parties and in the media.16 Through their company [company 1], they worked on the realisation of [crypto-system] .17 They rolled out the tool (in phases) and made it available to the public and remained intensively involved after its launch.

In other words, the accused, [co-defendant 1] and [co-defendant 2] are the inventors, creators and implementers of [crypto system] . As such, they are also responsible for the (consequences of the) operation of this tool. The autonomous, immutable and unstoppable nature of the smart contracts does not act as a disulpatory factor in this context. After all, this is not a fortuitous circumstance. These properties are the result of conscious choices made by the designers. [Crypto system] works as it was conceived. In the court's opinion, the accused can therefore be regarded as committing the money-laundering acts carried out by [crypto system].

The fact that third parties were also involved in the phase of development of the various functionalities does not alter the foregoing conclusion. Defendant, [co-defendant 1] and [co-defendant 2] formed the core of [crypto-system] as stated above.

Nor does the fact that [crypto-system] at some point started functioning as a so-called Decentralised Autonomous Organisation (hereinafter DAO) alter the foregoing. The court explains this as follows.

In December 2020, a proposal was adopted that transferred the governance of [crypto-system] to the community. [crypto-system] became a so-called DAO and was thus from then on under the leadership of the community.18

It follows, first of all, that up to that point, the governance was with the team, something the accused himself also confirms in his written statement.19

The court finds that handing over governance to the community was a deliberate choice by the defendant, [co-defendant 1] and [co-defendant 2] . They announce the [proposal] on 18 December 2020, introducing the TORN token.20 Their proposal is adopted and the [tokens] are created, 10 million in total.21

The [tokens] enabled holders to make proposals and exercise voting rights. Within the DAO, there are two ways in which proposals can be made and adopted, through on-chain governance and off-chain governance.

Larger strategic decisions are made through on-chain governance. Token holders can make their own proposals and vote on proposals. Proposals are posted on the [community] forum. Proposals are only implemented if on-chain governance rules are met. Those rules mean, for example, that you must have a minimum of 1,000 [tokens] to make a proposal, that you must lock the tokens and that a proposal cannot be adopted until at least 25,000 votes have been cast.

Less weighty decisions can be taken through off-chain governance. Off-chain governance takes place in a more informal setting. Making proposals and voting takes place via snapshot. Voting does not require [tokens] to be fixed and the number of votes required varies for each proposal.22

Whether the proposals were adopted through on-chain governance or through off-chain governance, in either case, it is true that in doing so, the core functioning of [crypto system] could not be modified, because of the immutable and autonomous smart contracts the tool was built with.23

Proposals that were adopted could thus only be implemented in future versions of [crypto-system] or concerned less essential functions that could be adapted. This fact in itself means that the fact that the governance of [crypto-system] was transferred to the community at some point does not constitute a shift of responsibility.

Moreover, the court deduces from the file and the proceedings at the hearing that there was no actual transfer of governance to the community either. This is because the aforementioned 10 million [tokens] , with which proposals could be made and votes could be cast, were distributed according to a certain system. This system led to a small group, consisting of the accused, [co-accused 1] , [co-accused 2] and two investors, receiving 30% of the 10 million [tokens].24 This meant that this small group, and thus also the accused, retained substantial control.

The court further notes that after handing over governance, the [crypto-system] team continues to play an important role in the further development of [crypto-system] . The defendant states that after handing over control to the community, the team remains the main supplier of ideas and codes.25 It also appears that in practice, only a limited number of people cast a vote on proposals made.26 This is addressed by the [crypto-system] team by not posting announcements of new proposals on public channels.27 There are also instances when the team decides on a modification in [crypto-system] that has not been submitted to the community at all.28

The court further finds that the defendant also had an interest in [crypto-system] being used by third parties. By introducing the TORN token, [crypto-system] became a source of income for its holders and therefore also for the defendant.29 The defendant therefore had a financial interest in the use of [crypto-system] by third parties.

Conclusion

In view of the above, in the opinion of the court, [crypto-system] cannot be seen as a stand-alone instrument separate from its inventors and creators; defendant, [co-defendant 1] and [co-defendant 2] . [crypto-system] functions as it was designed by them and in terms of its operation is entirely their responsibility.

- *Is there intent?*

For Section 420bis Sr to be proven, intent, whether conditional or not, is required. This means that it must be established that the accused knew or knowingly accepted the substantial likelihood that the Ether whose origin, movement and rightful owners were concealed or hidden, or in respect of which it was concealed or hidden who had it at his disposal, originated from crime.

The court finds that the accused had at least conditional intent to launder the Ether mentioned in the indictment and considers the following.

The significant probability.

The court has already established that [crypto-system] by its nature is eminently suitable for carrying out money laundering acts of concealment and disguise in the service of users who remain anonymous. This makes it evident that the use of [crypto-system] is very attractive for possessors of Ether with criminal origins.

It is a fact of common knowledge that similar services like [crypto system] are frequently used for money laundering. Already in 2014, a report was issued by the Financial Action Task Force (hereinafter: FATF) disclosing that mixers are used in crypto-currency laundering. The FATF explicitly states that a mixer is a tool to disguise the transaction chain on the blockchain. The FATF designates mixers as an indicator of money laundering and terrorist financing from 2020.30 The Financial Intelligence Unit-Netherlands (FIU) has also designated the use of a mixer as a money laundering indicator as of 15 August 2017.31

Although [crypto-system] differs somewhat from other services referred to as cryptomixers in its operation (because [crypto-system] does not mix the crypto-currencies deposited in the pools among themselves), the purpose of [crypto-system] is nevertheless similar to that of more traditional mixers. Namely, its purpose is to break the transaction trail on the blockchain. In the court's opinion, [crypto-system] thus falls equally within the definition of the term mixer used by the FATF and the FIU, so there is an increased risk of money laundering.32

That risk has subsequently manifested itself. Indeed, the file shows that [crypto system] was frequently used to launder Ether derived from crime. Looking at the Ether included in the indictment, 535,809 ETH came from hacks. This Ether has a total value of about USD 1.2 billion.33

However, because of the parameters used in the selection of hacks included in the indictment, this proportion is a lower limit. Indeed, only hacks in which more than USD 5 million was captured and disclosed to the public were taken into account in that selection. If those parameters are dropped, it becomes clear that the amount of Ether with a criminal origin deposited in [crypto system] is considerably higher. Then the total is USD 2.2 billion. That is almost 30% of all Ether deposited in [crypto-system].34 Moreover, it cannot be ruled out that crypto-currencies have also been laundered through [crypto-system] that were not obtained from a hack (theft), but from another crime (e.g. from trading illegal goods). In that case, the percentage is even higher.

Given all this, in the court's view, it was foreseeable from the beginning that Ether derived from crime would be deposited in [crypto system], due to the concealment effect of [crypto system] . This actually happened frequently and to a large extent. Concealment has de facto always been a core activity of [crypto system]. The likelihood that the Ether deposited in [crypto-system] would originate from crime was therefore significant.

Defendant was aware of the probable probability.

As indicated above, the Ether included in the indictment came from hacks that were disclosed to the public. Articles about these hacks were easy to find and in some cases those articles also mentioned the use of [crypto system] .35

The court notes that the defendant participated in several chat groups discussing the content of these articles and the fact that crypto-currencies with a criminal origin were deposited in [crypto system].36

One of the most notable chat conversations is one between the defendant, [co-defendant 1] and [co-defendant 2] , which shows that as early as 29 March 2022, the [crypto-system] team is made aware of the [internet site 30] hack, in which cryptocurrency worth around USD 600 million was stolen. Then, in the period from 5 April to 19 May 2022, the Ether captured in that hack worth almost USD 450 million passes through [crypto system] .37

Also found in the defendant's phone were several messages from police forces and private parties, requesting [crypto system] to assist in solving cases.
These involved cases involving stolen Ether that was subsequently deposited in [crypto system].38

Finally, the accused also states that he himself was familiar with articles stating that Ether derived from crime was deposited in [crypto system].39 He additionally states that the use of [crypto system] can lead to a so-called red flag at exchanges.40

Based on the foregoing, the court finds that the accused had knowledge of the fact that large quantities of felony-derived Ether were deposited in [crypto system]. In other words, he was aware of the substantial probability of this. That probable chance also extended to the Ether specifically mentioned in the indictment that originated from hacks.

Defendant knowingly accepted the substantial opportunity.

The foreseeability and knowledge of the large-scale abuse of [crypto-system] did not prevent the defendant from developing [crypto-system] and offering it to the public without limitation (e.g. by incorporating compliance measures). On the contrary, the defendant continued to design and roll out [crypto-system] despite that foreseeability and knowledge, with almost every follow-up step reinforcing the concealment and anonymity of users.

As pointed out above, the defendant developed the pools' smart contracts together with the team, as well as the UI and the relayer software. In the court's view, these are the core functions of [crypto-system] and all these functions harbour elements that prioritise the user's anonymity and thus enhance the concealment effect of [crypto-system]. The court discusses these below.

There were several pools into which users could deposit their cryptocurrency. The 100 Ether pool was the largest. Although a highly fluctuating value is characteristic of cryptocurrencies, the 100 Ether pool was attractive from the start for the user with a large amount of Ether on hand.
This also makes this pool ideally suited to users looking for a way to launder large quantities with criminal origins. After all, the pool makes it possible to move large amounts of Ether in fewer transactions. Consequently, this pool was by far the most commonly used when depositing the charged Ether.41

The UI provides any user with easy access to the smart contracts of the pools of [crypto system] . Such access is not accompanied by any know your costumer" (KYC) functionality. Both when depositing and withdrawing cryptocurrencies, no identifying information needs to be provided . Also, no Know Your Transaction (hereinafter KYT) verification takes place . Therefore, [crypto system] does not create any barrier for the user who has criminal assets and wants to launder these assets.

[Crypto system] has had several relayer functions. The file shows that the defendant creates and publishes the first version of the relayer system. In subsequent years, too, it is the defendant who is the most active developer of the relayer function.42 The defendant himself also states that he made a substantial contribution to the relayer function.43

The last relayer version was activated in February 2022, the relayer registry said. Research into the use of this functionality shows that users made frequent use of it, including users in possession of stolen Ether. With regard to two hacks included in charges the [company 2] Hack and the [internet site 30] hack, it was found that relayers were used to record the cryptocurrency stolen with those hacks.44 Therefore, this feature is also gratefully embraced by users with criminal intentions.

In May 2020, on the initiative of the [crypto system] team, a Trusted Setup ceremony took place where the operator address of the pools' smart contracts was set to 0. This gave up any form of control over these smart contracts.45 Even the verifier, a smart contract that checks whether the instruction for recording is correct (zero-knowledge proof), could not be changed from then on.46 Users were thus assured of complete anonymity, with no risk of human interference. The defendant is one of those who contributed to this.47

Finally, at no point did the defendant disassociate himself from [crypto system] despite his knowledge of the deposits of criminal assets into [crypto system] . Until the day of his arrest on 10 August 2022, he remained actively involved in [crypto-system].48

Intermediate conclusion.

The court notes that from the beginning, the goal was to develop the best possible privacy solution for the user, despite the fact that Ether derived from crime was deposited in [crypto-system] on a large scale. During the conception, development and roll-out of [crypto-system], the choice was made time and again to make the use of [crypto-system] more attractive to every user, including the criminal user. Securing user anonymity and concealing transaction history have remained central.

Until the moment of his arrest, the defendant continued to work on improving the privacy solution that [crypto-system] intended to provide. A moment when the defendant no longer wanted to be associated with [crypto-system] did not come. The defendant took the easy, unlimited, foreseeable and obvious use of [crypto-system] by criminals at face value.

The court concludes that the accused knowingly accepted the substantial probability that the indictable, felony-derived Ether was deposited in [crypto system], making him guilty of its laundering.

- *Are there any contraindications showing that conscious acceptance does not exist?*

The defence disputes that there was an acceptance of probable cause. To that end, the defence first argues that the development and implementation of the compliance tool in [crypto system] precludes the assumption of conditional intent. Indeed, this shows that the probability of a criminal origin of crypto-currencies was not taken at face value, but rather
has been expressly opposed. This also applies to the application of the [system] . Other facts and circumstances also show that there was no conscious acceptance.

The court will discuss below the compliance tool, the [system] and the other facts and circumstances presented.

The compliance tool.

The compliance tool will be introduced in June 2020. This tool will enable the user of [crypto system] to demonstrate the transaction history of the cryptocurrency if necessary, for example because an exchange requests it.49

The court noted that the use of the compliance tool is an entirely voluntary choice of the user. If the user does not want to use the tool, for instance because it would become provable that the cryptocurrencies came from a hack, he will not use the tool. The user will then simply have to exchange or cash his cryptocurrency by some means other than through an exchange that insists on proving the transaction history.

[crypto system] cannot in any way apply the compliance tool itself. The information that can be demonstrated by the compliance tool by the user is not available to [crypto system] .50

This means that the compliance tool is only a relevant tool for the user of [crypto system] who records cryptocurrencies that come from a legitimate source. However, the compliance tool in no way makes [crypto system] less attractive to the non-legitimate user.

In view of this, the court finds that the development of the compliance tool does not show that the accused did not accept the laundering by [crypto system]. The compliance tool is useful for the user with legitimate intentions, but it does not impose any restriction on the user with illegal intentions.

The [system] .

On 15 April 2022, [crypto-system] publicly discloses that it uses the [system] to monitor transactions.51 The [system] contains a list of sanctioned wallet addresses and can be used to bar those sanctioned addresses.52 Investigations revealed that the source code of [crypto-system]'s UI contains the script that checks whether an address is sanctioned.53

While at first glance the implementation of the [system] does indeed appear to be a form of a KYT control by which [crypto system] aims to prevent abuse, in reality the implementation has little effect. This was also obvious to the defendant. He states that it was clear in advance that the implementation of the [system] , would not be able to deter hackers from using [crypto-system] misuse.54 Bypassing the [system] is easy by not connecting to the UI of [crypto system] with a sanctioned address, but by doing so via one or more intermediate addresses. On top of that, the source code of the UI is public, so third parties can use it and easily modify it so that the check by the [system] does not take place.55

In view of the above, the court finds that the implementation of the [system] does not show that the defendant did not accept the laundering by [crypto-system]. The tool was unsuitable to prevent the misuse of [crypto-system] and the defendant was aware of this when it was implemented.

Other facts and circumstances.

The defence put forward that, due to the technology of [crypto system] , the defendant had no effective means to act against the misuse of [crypto system] . The court considered as follows.

In this regard, the court first of all states, as it has already considered above, that this is a circumstance created by the defendant himself and that to that extent that circumstance is not exculpatory . [crypto system] operates in the way it was designed by the defendant. If the defendant had wanted to have possibilities to act against possible abuse, the defendant should have built in those possibilities.

The defendant could also have distanced itself from [crypto-system] by no longer promoting its use and emphatically pointing out that it was being misused. However, at no time did the accused report to authorities that Ether derived from crime was being deposited in [crypto-system] or take any other action. On the contrary, the defendant, [co-defendant 1] and [co-defendant 2] only drafted a general message which they sent to authorities and individuals asking for help if it turned out that their stolen Ether had been deposited in [crypto-system].56 The message made it clear that the [crypto-system] team could do nothing for them.

The defence further argues that the team sought legal advice. This would also show that there was no deliberate acceptance of probable cause. The court notes the following.

Indeed, the defendant states that he, [co-defendant 1] and [co-defendant 2] sought legal advice on [crypto-system] . The outcome, according to the defendant, was that [crypto-system] was not covered by FinCEN regulations and that there was no obligation to build compliance measures into [crypto-system].57 The defendant also states that he was therefore under no obligation to report, for example, that Ether derived from crime was deposited into [crypto-system].58

However, the court considers that the question of whether or not [crypto system] is a financial institution required to comply with compliance regulations is irrelevant. What matters is whether the defendant and its associates complied with the law. Compliance with compliance regulations serves the prevent violations of law, but not being subject to compliance rules does not relieve anyone of the obligation to comply with the law. No one may engage in money-laundering conduct that is punishable by law. The accused's team violated this rule.

Finally, the defence argued that the accused acted in full publicity and was publicly known as one of the developers of [crypto-system] . According to the defence, this too would show that there was no conscious acceptance of the misuse of [crypto-system]. The court considers the following in this regard.

The court notes that the team has always stressed that in developing [crypto system] , it had in mind the preservation of privacy when making transactions on the Ethereum blockchain. In pursuing that goal, the team always deliberately put the ideology of maximum privacy ahead of other interests, such as the integrity of financial transactions, the right to property and the importance of detecting crimes. However, acting from an ideology does not make you untouchable from laws and regulations that apply to everyone, even when doing so in full transparency.

Conclusion.

Contrary to the defence's contention, the court finds that there are no facts and circumstances present that preclude the assumption of conditional intent. The court therefore upholds its conclusion that the accused knowingly accepted the substantial likelihood that Ether derived from crime would be deposited in [crypto system], the origin, movement and rightful owner of which would subsequently be concealed or disguised, so that he and his co-perpetrators were guilty of laundering it.

- *Is there co-perpetration?*

The court first states that involvement in an offence in the form of co-perpetration can be proven if it has been established that there was sufficiently close and conscious cooperation in its commission.

From the file and the investigation at the hearing, the court deduces the following with regard to the involvement of the accused and others in the charges. The accused together with [co-defendant 2] and [co-defendant 1] formed the [crypto-system] team. They are the founders of [crypto-system] and ensured that [crypto-system] functions as it does.59

On the basis of the above, the court finds that there was close and deliberate cooperation between the accused and his co-perpetrators consisting, in essence, of joint execution. That cooperation lasted throughout the entire period charged. This means that the accused and his co-perpetrators can be regarded as co-perpetrators of the money laundering offences charged throughout the entire period of the indictment.

- Habitual whitewashing.

The court finds legal and convincing evidence that the accused and his co-perpetrators laundered Ether originating from 36 individual hacks via [crypto system] over a period of more than two years.

They thereby committed money-laundering acts over a long period of time and at a high frequency, so that these behaviours should be classified as habitual. The court therefore qualifies the actions of the accused and his co-perpetrators as co-perpetration of habitual money laundering.

Final conclusion.

The court considers it legally and convincingly proven that the accused, together with others, was guilty of laundering the Ether from crime listed in the indictment and that he made this laundering a habit.

5 The statement of evidence.

Based on the facts and circumstances contained in the evidence annex and articulated in the evidence recital, the court concludes that it has been legally and convincingly proven that the accused:

on one or more occasions during the period from 9 July 2019 to 10 August 2022 in the Netherlands and in Russia and/or the United States and/or in Dubai, together and in association, made a habit of committing money laundering,

After all, the accused and his co-perpetrators of objects, namely 535,809 crypto currency (ETH) (worth approximately $1,217,343,820), consisting of
- 50,930 ETH (sourced from [internet site 1])
- 7,466 ETH (sourced from [internet site 2])
- 14,012 ETH (sourced from [internet site 3])
- 2,420 ETH (sourced from [internet site 4])
- 2,994 ETH (sourced from [internet site 5])
- 6,628 ETH (sourced from [internet site 6])
- 2,410 (taken from [internet site 7])
- 7,204 ETH (sourced from [internet site 8])
- 2,037 ETH (sourced from [internet site 9])
- 4,004 ETH (sourced from [internet site 10])
- 5,855 ETH (sourced from [Internet site 11])
- 8,264 ETH (sourced from [internet site 12])
- 2,026 ETH (sourced from [Internet site 13])
- 17,181 ETH (sourced from [internet site 14])
- 3,223 ETH (sourced from [internet site 15])
- 2,023 ETH (sourced from [internetsite 16])
- 4,900 ETH (sourced from [internet site 17])
- 9,300 ETH (sourced from [internet site 18])
- 2,200 ETH (sourced from [internet site 19])

- 30,397 ETH (sourced from [internet site 20])
- 2,560 ETH (sourced from [internet site 21])
- 1,971 ETH (sourced from [internet site 22])
- 7,500 ETH (sourced from [internet site 23])
- 2,794 ETH (sourced from [internet site 24])
- 10,290 ETH (sourced from [internet site 25])
- 2363 ETH (taken from [internet site 26])
- 2,116 EHT (taken from [internet site 27])
- 8,801 ETH (sourced from [internet site 28])
- 4,566 ETH (sourced from [internet site 29])
- 175,100 ETH (sourced from [internet site 30])
- 24,849 ETH (sourced from [Internet site 31])
- 5,446 ETH (sourced from [internet site 32])
- 3,931 ETH (sourced from [internet site 33])
- 85,700 ETH (sourced from [internet site 34])
- 7,561 ETH (sourced from [internet site 35])
- 4,787 ETH (sourced from [internet site 36])
concealed or disguised the origin and movement and concealed or disguised who the rightful owners of the objects were and concealed or disguised who held the objects,

while the accused and his co-perpetrators knew in each case, that the objects were entirely immediately or indirectly - derived from any crime.

6 The criminality of the act.

The proven offence provides the offence stated in the judgment.

No facts or circumstances have become plausible to rule out the punishability of the offence.

7 Defendant's criminality.

No facts or circumstances have become plausible that preclude the defendant's punishability. Defendant is therefore punishable for what has been proved.

8 Imposition of punishment.

<u>The prosecution's claim.</u>

The prosecution is demanding a sentence of 64 months' imprisonment less remand in custody.

In addition, the prosecution claims the forfeiture of:

- the Binance credit (No 1, KVI-008, value 1,026,440.00);
- USDT credit (No 5, Tether, RHV, USD 233,360, estimated value 212.358,-);
- the [tokens] received at the beneficiary address [address] (No 6, FIN-006, 388.358.8611 [tokens] , estimated value approximately 629,064);
- the balance in a Swiss bank account held by the defendant (No 7, RHV, 36,449.00);
- the Porsche including registration certificate and keys (no. [number] , value 75.295,76).

A copy of the prosecution's claim and a copy of the attachment summary are attached to this judgment.

<u>Defence position.</u>

The defence pleaded acquittal and no sentencing defence.

With regard to the seizure, the defence requests the return of these items to the accused as they are not from any crime.

<u>The court's verdict.</u>

General.

In deciding on the punishment to be imposed on the accused, the court took into account the nature and seriousness of the proven offence and the circumstances under which it was committed. In assessing the seriousness of the offence committed by the accused, the court takes into account the statutory maximum penalty and the penalties imposed for similar offences. In addition, the court takes into account the defendant's person and personal circumstances when determining the punishment.

Seriousness of the fact.

Defendant, together with others, was guilty of habitually laundering large amounts of Ether representing a high financial value. That laundering took place through the tool [crypto system] developed and maintained by the accused and his co-perpetrators. The Ether mentioned in the statement of evidence constitutes a fraction of the whole. In total, more than US$2 billion (converted) was laundered using [crypto-system].

The tool developed by the defendant and his co-perpetrators combines maximum anonymity and optimal concealment techniques on the one hand, with a serious lack of functionalities enabling identification, monitoring or detection on the other. Accordingly, [crypto system] cannot be characterised as a legitimate tool unintentionally misused by criminals. By its very nature and operation, the tool was intended for criminals. The defendant and his co-perpetrators designed the tool so that it automatically performs the concealment operations essential for money laundering. The criminal user is completely unburdened. The user asks, [crypto system] runs, no questions asked. It must be a nightmare for the legitimate possessor of cryptocurrencies that hackers can make themselves and the assets they have stolen invisible and untraceable thanks to [crypto system] .

It goes without saying that the laundering of cryptocurrencies leads to disruption of economic and financial traffic. The laundering of crypto-currencies derived from crime brings them into the legal traffic without this being apparent to (bona fide) participants in the traffic. Individuals and companies, including financial institutions, thus become involved in the actions of criminals. This causes serious damage to the integrity of the financial and economic system.

Through the development and launch of [crypto-system], the defendant and his co-perpetrators have been of great value to the underworld, with the eye-catching low point being the [company 3] hack committed by the [hacker group] , in which USD 625 million of crypto-currency was stolen. Of this, nearly USD 450 million in Ether was deposited into [crypto system] and laundered. The [hacker group] is associated with (financing) the North Korean regime.

With regard to privacy, the accused and his co-perpetrators sought to draw a parallel between cryptocurrency transactions on the blockchain, on the one hand, and transactions in the banking world, on the other. However, in doing so, they failed to provide safeguards to protect the integrity of the financial and economic system, as is common and even mandatory in the banking world. The accused and his co-perpetrators thereby developed a privacy tool that created a shortcut for financing crimes, totalitarian regimes and terrorism. A shortcut created in such a way that it is immutable and unstoppable.

Under the guise of an ideology, the defendant has evaded laws and regulations that apply to everyone and has thought himself untouchable. He has behaved lazily when requests for help from victims of hacks or investigative agencies came to him, simply stating that he could do nothing for them. With blinders on, completely ignoring the abuse that took place via and through [crypto system], he continued to develop and exploit this service. The defendant chose to look away from the abuse and not take any responsibility for it. Meanwhile, the defendant did manage to enrich himself with his concealment service for criminal assets.

All this, the court charges the defendant very much.

Forfeiture.

The court finds that the seized items under numbers 1, 5 and 9 of the seizure list and the unseized items under numbers 6 and 7 of the seizure list are liable to forfeiture, because - as evidenced by the investigation at the hearing - these are items that belonged to the convict and were obtained entirely through the offence.

The court will order the return to the accused of the seized items under numbers 2, 3 and 4 of the seizure list, as no relationship can be established between these items and the offence. In view of the fact that these goods have also been seized on a precautionary basis, this decision will not result in the actual return of the objects.

The court refrains from ruling on the object listed under number 8 on the seizure list. This object has not been seized, and while this need not preclude forfeiture, there is no basis for it in this case.

Conclusion.

Weighing all the facts and circumstances against each other, the court is of the opinion that, in connection with proper law enforcement, it is not sufficient to impose a different or lesser punishment than the requested prison term of 64 months, minus the remand in custody.

Enforcement of the prison sentence to be imposed will take place entirely within the penitentiary, until the moment the accused is granted conditional release as referred to in Article 6:2:10 of the Code of Criminal Procedure.

9 Applicable articles of law.

The decision is based on sections 33, 33a, 34, 47, 63, 420bis, 420ter of the Penal Code.

THE EXECUTION

The court:

- Declares the charges proven as described above;

- declares not proven what the accused has been charged with more or otherwise than has been proved above and acquits him thereof.

The proven fact delivers on the crime:

Complicitly making a habit of committing money laundering.

The court declares the accused punishable for this and imposes the following punishment:

- A sentence of **64 months' imprisonment** with deduction of remand in accordance with Article 27 of the Penal Code.

- **Forfeiture** of the seized items, viz:

o 1,026,440.00 (Binance credit), KVI-008, **no. 1** of the attachment summary;

o 233,360 USDT (Tether), RHV, estimated value 212,358, **no. 5** on the batter's list;

o 388,358.8611 [tokens] (received at the [address] beneficiary address), FIN-006, estimated value 629,064.00, **no. 6** of the attachment schedule;

o 36,449.00 (balance in Swiss bank account), RHV, **no. 7** of the attachment schedule;

o Porsche (including registration certificate and keys), KVI-007, **no. 9** of the attachment summary.

The court orders the return to the accused of the items seized from him, namely:

o 16,302.00 (Trustwallet), KVI-004, **no. 2** of the attachment summary;

o 62,198 (Private keys phone), KVI-003, **no. 3** of the attachment summary;

o 81,039.00 (TC Notes and private keys MacBook), KVI-010, KVI-011 and KVI-012, **no. 4** of the attachment summary.

This judgment was delivered by:
Mr H. Slaar, chairman,
M.J.M.A. van der Put and R. van den Munckhof, members, in
the presence of N.P.M. van de Wouw, registrar, and was
pronounced on 14 May 2024.

[1] DOC-156, page 01A0635 and ZD-001, page 109.

[2] See, for example, ECLI:NL:GHDHA:2020:1804.

[3] AMB-075a, DOC-033a, page 3263 and AMB-087, page 01A0526.

[4] TK 1999-2000, 27159, no. 3, p. 4.

[5] TK 1999-2000, 27 159, no. 3, p. 14.

[6] TK 2000-2001, 27 159, no. 7 page 1.

[7] DOC-064, page 3386.

[8] Defendant's statement at the court hearing on 26 March 2024.

[9] AMB-011 sets out the operation of [crypto system].

[10] ZD-001, page 96.

[11] AMB-001, pp. 264 and 265 and DOC-064, 3417.

[12] AMB-001, page 258.

[13] AMB-064 explains the operation of relayers.

[14] AMB-019, page 361.

[15] Defendant's statement made at the hearing dated 26 March 2024.

[16] AMB-014, page 345 and ZD-001, page 94.

[17] AMB-019, page 363 and V-001-10, page 01A0104.

[18] AMB-022, page 385.

[19] V-001-09a, page 01A0080.

[20] DOC-064, page 46.

[21] DOC-102.

[22] AMB-062, pp. 619 and 620.

[23] V-001-09a, page 01A0081.

[24] AMB-022, page 401.

[25] V-001-07, page 01A0043.

[26] AMB-062, pp. 625 and 626.

[27] AMB-022, page 396.

[28] AMB-062, page 665.

[29] AMB-057, pages 577 and 578, AMB-057a, pages 582 and 583 and AMB-062, page 617 and the statement of
Defendant deposed at the hearing dated 26 March 2024.

[30] ZD-001, page 94.

[31] AMB-001, page 266.

[32] ZD-001, page 95.

[33] ZD-001, page 108.

[34] AMB-97, pp. 01A579 to 01A580.

[35] AMB-042 and AMB-075a.

[36] AMB-043 and AMB-014.

[37] ZD-001, page 110 and AMB-043, pages 509 and 510.

[38] AMB-055.

[39] V-001-02, page 168.

[40] V-001-07, page 01A0035.

[41] AMB-075a, page 776.

[42] AMB-019, page 361.

[43] V-001-07, page 01A0035.

[44] AMB-064, pp. 683, 687 and 696.

[45] V-001-11a, part 5.

[46] AMB-077, pp. 789 and 790.

[47] AMB-062, page 615.

[48] AMB-069, page 746.

[49] AMB-062, page 616.

[50] Statement of the accused made at the hearing dated 26 March 2024.

[51] DOC-031.

[52] AMB-043, page 508.

[53] AMB-066, pp. 701 and 702.

[54] V-001-13a, page 01A0045.

[55] AMB-066, page 703.

[56] DOC-040, page 3313.

[57] V-001-13b, page 01A0452.

[58] Statement of the accused made at the hearing dated 26 March 2024.

[59] V-001-10 and AMB-019, pp. 361 and 363.