Anti-Money Laundering efforts in The Netherlands – Part I 'The Dutch Model'
Prepared by dr. R.S. van Wegberg, Delft University of Technology, the Netherlands

Introduction
Criminal misuse of the financial system is intrinsic to money laundering and the primary focus of governmental anti-money laundering efforts. While the fight against crime historically takes place in the well-known policy circles of criminal justice – i.e., law enforcement and the judiciary – anti-money laundering efforts involve yet another branch of government. Given the considerable involvement of the financial system in money laundering, the Treasury is also part of the governance structure against money laundering. This attempt to converge these three distinct governance perspectives in the Netherlands is made mainly through legislation – e.g., regulation.

Initially, anti-money laundering efforts were handled through legislation in two respects. First and foremost, in the financial system, financial service providers are required to know who they were dealing with. That is, the client's identity had to be established. This resulted in the Identification of Services Act (in Dutch: Wet Identificatie Dienstverleners) in which regulations were laid down for the Dutch implementation of what is commonly called Know-Your-Customer (KYC). Before a client can gain access to services of a financial service provider, his identity had to be established. Second, the financial service provider is required to assess whether its client is engaged only in legitimate matters, requiring that they report any unusual transactions. These rules were laid down in the Disclosure of Unusual Transactions Act (in Dutch: Wet Melding Ongebruikelijke Transacties), which stipulated that transactions that met certain conditions and could therefore be seen as a risk, had to be reported to a reporting body. This notification obligation would be supervised by four supervisory authorities, identified below.

After amending this legislation a number of times in response to societal developments, resulting in the imposition of stricter requirements on client due diligence as well as an increase in the number of institutions required to report, the Dutch government concluded that these two separate laws impeded the implementation of both aspects of their anti-money laundering efforts. Institutions – like banks – were required to review two sets of regulations to which they were subject resulting in a lack of clarity about the complete spectrum of their legal obligations. To address this problem, the Dutch government merged this twofold legislation into the new Money Laundering and Terrorist Financing Prevention Act (in Dutch: Wet ter voorkoming van witwassen en financieren van terrorisme; short Wwft). This merger provided an opportunity to set clear rules and instructions regarding customer due diligence and reporting obligations with regard to unusual transactions in a holistic and uniform manner. The bill to merge received support in both Houses of Parliament and was passed in the Senate on May 22nd 2008.

Governance structure
The fight against money laundering balances the governance perspective of the police and the judiciary on the one hand and that of the financial system on the other. The departments responsible must jointly coordinate and steer anti-money laundering efforts and have assigned responsibilities to various government actors and outlined their mutual relationships. This creates the Dutch structure within which anti-money laundering governance should take place. The various organizations within this structure are not solely dedicated to anti-money laundering and have other responsibilities alongside those assigned to them as well. The anti-money laundering tasks to be performed by these organizations can be divided into three core activities: 1) reporting and preventing of money laundering, 2) detection and prosecution of money laundering, and 3) sanctioning of money launderers. These three elements will be discussed in turn below.

Prevention of money laundering is primarily based on gaining insight into the nature, size and scope of money laundering activity. Once the nature and scope of the problem is understood, tailor-made measures can be applied faster and to greater effect. Transparency in the financial system is also a form of prevention. If it is easier to 'see' that the financial system is being misused for illegal activities, one can intervene swiftly and adequately. Prevention also includes criminalizing money laundering, which – at least theoretically – should act as a deterrent to potential money launderers. It is also important to increase the likelihood that money laundering activity will be detected and those involved caught. Understanding how frequently unusual activity is reported also assists in evaluating the efficacy of the governance structure, as well as assessing the scope of money laundering and the number of people involved. potential amount of money launderers.

The importance of reporting in the Dutch system should not be overlooked. In the Dutch approach against money laundering, reporting can be described as the corner stone of the governance structure - without reporting of unusual transactions, all other efforts will have limited to no effect. The notification and identification obligation briefly discussed above, provides the majority of reports. As described above, financial service providers are required to identify their clients before they have access to their services and are required to report unusual transactions to a reporting body on the basis of certain indicators. These indicators can be differentiated between subjective and objective indicators. The former are transactions that stand out because they are unusual . The classification thereof as "unusual" is entirely the responsibility of the reporting institution – e.g., a bank. Hence this is also called the subjective indicator. This means that institutions themselves assess the risks associated with certain clients or products and adapt their efforts accordingly. This approach can be specified in sectoral compliance regulations, but it is always the institution's own responsibility and duty of care to follow these (sectoral) regulations. Accordingly, the Wwft does not prescribe *how* an institution must achieve something, but only *what* must be achieved – i.e., the reporting of unusual transactions.

Objective indicators cover all transactions with a value of (converted) € 15,000. Regardless of whether any subjective indicator is present, an institution must report all transactions above € 15,000 to the Financial Intelligence Unit-Netherlands (FIU-the Netherlands). Institutions obliged to report unusual transaction, are private parties such as:

1. financial service providers – like banks, insurers, casinos, credit card companies;
2. dealers in valuables – like real estate agents;
3. lawyers, civil-law notaries, accountants, tax advisers;
4. investment institutions, insurance brokers.

For each group of institutions, a supervisor has been appointed by the Treasury, who is responsible for ensuring that clients of those institutions are identified and unusual transactions are reported. The first group is under the supervision of the Dutch Central Bank (DNB), the second group of the Tax and Customs Administration, the third of the Financial Supervision Office (BFT) and the fourth of the Netherlands Authority for the Financial Markets (AFM). All are under the responsibility of the Treasury, with the exception of the BFT, which is the responsibility of the Justice department. In addition to reports from the reporting institutions, reports are also submitted by investigative authorities and other government services. On Amsterdam Schiphol Airport, for example, the Royal Netherlands Marechaussee (KMar) and Customs, report unusual 'transactions' – like large amounts of cash – as part of their general duties.

Reports of money laundering can lead to an investigation by law enforcement in two ways. The first route is through FIU-the Netherlands. In this case, an alert is sent out by an institution obligated to report, after which FIU-the Netherlands examines and analyzes whether these data merit a follow-up investigation. If this is the case, a law enforcement agency can use the enriched information from FIU-the Netherlands to initiate an investigation. The FIU-the Netherlands does not play a role in the second route. In the second route, reports originate from law enforcement itself and they will then proceed to investigate further. This provides Dutch law enforcement with the opportunity to start their own investigation without receiving information through the FIU-the Netherlands and/or relying on reports from private parties. In addition to the police, the Fiscal Intelligence and Investigation Service (FIOD) is specifically tasked with investigating money laundering in the Netherlands.

Objectives and priorities
As the Justice department bears primary responsibility for the fight against crime, the fight against money laundering is included in their annual budget. The Treasury have set a number of objectives and priorities regarding the anti-money laundering efforts in their annual policy documents. The objectives are:

- Prevent and counter integrity violations at financial institutions including clients misusing financial institutions to launder money;
- Detect and prosecute organized crime effectively and efficiently.

In order to meet these objectives, the following priorities are identified:

- Decrease the amount of criminal assets;
- Initiate investigations of financial-economic crime;
- Financial investigation must be an integral part of any substantial investigation by the police and / or the special investigative services into serious or organized crime;
- As much as possible, the police, the special investigative services and the Public Prosecution Service conduct investigations in response to suspicious transactions submitted to FIU-the Netherlands;
- When large amounts of cash or other unusual assets are found, an investigation should be carried out into the origin of the cash or assets as often as possible.

These objectives are in line with European and/or international guidelines and treaties to which the Netherlands adheres. The two main guidelines are those of the Financial Action Task Force (FATF) on Money laundering and the European Union directives to prevent the misuse of the financial system for money laundering and terrorist financing – i.e., the EU Money Laundering Directives 1-5.

Role and mandate of the FIOD

The Fiscal Intelligence and Investigation Service (FIOD) is one of the four special investigative services in the Netherlands. The organization focuses specifically on detecting and combating tax and financial fraud, including money laundering and corruption. The FIOD is tasked to assure a financially secure Netherlands. The organization joins forces with partners at home and abroad. The FIOD has three strategic objectives:

1. Investigations with maximum societal impact;
2. Fighting fraud through public-private partnerships;
3. Seizing criminal assets – crime shouldn't pay.

The FIOD is part of the Tax and Customs Administration, which is a special division of the Treasury. The organization has thirteen branches, spread over six regions. These regions each have their own specialty. For example, the theme of synthetic drugs is housed in the Southeast, and real estate in the Northwest region. Each region has different investigation units, including a Special Affairs team (BZT), a Money laundering team and a Multidisciplinary team (MDT). The BZT teams focus on major cases, such as international fraud schemes and investigations with a major financial impact, such as large-scale construction fraud that can go on for years occupy years, the MDT teams focus on relatively small investigations that last a maximum of one year.

The type of investigations carried out by the MDT are very broad: from tax and benefits fraud, money laundering and corruption to the trade in counterfeit goods. In addition to these investigation units, the FIOD has several specialist teams, including the Anti-Corruption Center (ACC), the Financial Advanced Cyber Team (FACT) and the Forensic IT Team (FITT). The FIOD also has its own Criminal Intelligence Team (TCI), an arrest unit (Team Special Assistance - TBB) and an observation team (Team Investigation Support - TOO).

Currently, the FIOD is staffed by around 1,400 employees – the majority of whom are law enforcement officers. The staff has a diverse range in background. Historically, the FIOD was staffed by lawyers, accountants and traditional law enforcement officers. Nowadays, most have an academic background in law, finance, criminology, computer or data science or are trained as forensic experts. After joining the FIOD, the majority are then trained as law enforcement officers, so they are also operational and can go into the field. Teams ranges in size between 10 and 30 people, depending on the region and task.

The FIOD also participates in the Anti Money Laundering Centre (AMLC). This national centre of expertise was established in 2013 to intensify the fight against money laundering at home and abroad. The AMLC functions as a meeting place for the FIOD and partners such as the police, the Public Prosecution Service (OM) and the Financial Intelligence Unit-Netherlands (FIU).

Role and mandate of the Dutch Anti-Money Laundering Centre

Combating money laundering is a priority for the Dutch government. In order to follow through on this priority, the Treasury has intensified its financial support to government actors involved in the fight against money laundering. To structure this effort, the Dutch government initiated the creation of an Anti-Money Laundering Centre (AMLC). The AMLC was established in 2013 to develop into a platform where parties involved in the fight against money laundering can share knowledge and experiences, but also cooperate operationally. Hence, the AMLC is a knowledge and expertise center where public and private parties work together to combat money laundering nationally and internationally. Public partners include the police, the Public Prosecution Service, the Financial Intelligence Unit (FIU), regulators, the FIOD and other special investigative services. Private partners include banks, accountancy firms and civil-law notaries. At the AMLC these parties join forces to contribute to the fight against money laundering and to protect the integrity of the financial system. For example, the AMLC formulates new money laundering typologies and discerns new money laundering modus operandi. Through special projects and large money laundering investigations a unique data position is built and managed. The AMLC currently

employs about 35 specialists from all kinds of organizations. Most of them are employed by the FIOD and seconded to the AMLC.

Since its foundation in 2013, the AMLC has gone through various stages of development. After being primarily concerned with reports of money laundering, this task was eventually assigned to the various FIOD investigation teams in the country. This allowed the AMLC to develop into a knowledge and expertise center. with the insight and knowledge developed by the AMLC, investigative questions can be adequately addressed and transactions can be better interpreted. The AMLC therefore actively shares knowledge and brings together the Dutch anti-money laundering governance structure.

Assessment of the effectiveness and the strengths and weaknesses of the Dutch approach to policing money laundering and financial crime

With the Wwft, the Netherlands has created legislation to prevent money laundering and terrorist financing. A number of government actors are tasked with executing this policy. The Wwft is based on two pillars. These pillars correspond to the responsible departments and the two objectives of the Wwft. The first of these responsible departments is the Justice department, with the objective of detecting and prosecuting organized crime effectively and efficiently, and the second is the Treasury, with the objective to prevent integrity violations at financial institutions and preventing clients from misusing financial institutions to launder money. This division creates a lack of clarity as to whom is in charge of and coordinates the execution of the Wwft – as both departments are responsible for various actors within the Wwft. From a legal point of view, the Treasury is the first signatory to the Wwft, and therefore responsible for the governance structure as a whole. While the Treasury has a strong understanding of the financial system, the same cannot be said about policing money laundering.

To counteract part of this uncertainty in roles and mandate of government actors, the AMLC was established in 2013. Since its inception, it has functioned as a bridge between all relevant government actors and stakeholders. Although not all perspectives can be aligned, the AMLC served a clear purpose. That is, relying on experts from public and private partners to literally join forces and work as one to counter money laundering in the Netherlands. In this way, part of the disconnect between actors in the financial system and law enforcement agencies investigating money laundering has been remediated. Note however, that a lot of operational results still stem from interpersonal relations and informal conversations and are not legally incentivized.

In addition to a lack of clarity that hinders cooperation between actors in the governance structure, the performance culture also plays a prominent role. Drawing up performance indicators for government actors incentivizes them to prefer not to share information – as closing cases single-handedly achieves individual targets. This also means the information available through the FIU is not used to its full potential. Investigations now mainly take place on the basis of information generated by the investigating agency, sometimes by means of residual information from other criminal investigations, but little to none on the basis of information available through the FIU. Moreover, the use of information from the FIU is not registered, so that it remains unclear in which cases information from the FIU was used. Moreover, there is no mandatory feedback from investigative authorities to the reporting body if their information has been used. This creates even more friction, as the FIU has no obligation to inform a reporting institution if their alerts have served as a basis for further investigation. If reporting institutions knows that their reports are leading to investigations, they will be more eager to comply with their reporting obligations.

Because there is no feedback throughout the governance structure, there is also no clear indication to its efficacy.

That law enforcement agencies mostly rely on their own information to initiate investigations into money laundering means two things. First, this creates a rich information position at several specialized units within both the police as the special investigation services – i.e., the FIOD. Second, this translates to in-depth expertise across these specialized units – e.g., dedicated financial cybercrime specialists or financial investigators in organized crime units.

Anti-Money Laundering efforts in The Netherlands – Part 2 'Research collaboration FIOD'

Prepared by dr. R.S. van Wegberg, Delft University of Technology, the Netherlands

Background

In the academic year 2018-2019, three Delft University of Technology graduates worked on a successful pilot project, researching relevant topics related to FIOD priorities. In the pilot project, the students focused on 'underground markets' – e.g., markets for illegal narcotics, cybercrime toolkits or money laundering services. They mapped their nature and size and examined the actionable perspectives for the FIOD in general and the Financial Advanced Cybercrime Team (FACT) in particular. After mutual enthusiasm about this ad-hoc collaboration – both thematically and personally – the desire arose to structurally strengthen this collaboration, both in duration and intensity. Here, we describe its current content, aim and impact.

Financial cybercrime

Professional facilitators are of vital importance to cybercriminals, as well as to effectively combatting financial cybercrime. On one hand, they lower the knowledge threshold for aspiring cybercriminals by making services available that would otherwise be inaccessible, such as cryptocurrency money laundering service providers, also known as bitcoin mixers. On the other hand, successfully targeting a bitcoin mixer could not only disrupt a wide range of criminal activities, but also enable data-driven follow-up investigations. This innovative approach to combatting financial cybercrime is one in which the FIOD, among others, is pioneering. Policing with impact is the guiding principle. But how does one achieve the greatest possible impact through such a strategy? Both with an operation itself, and with the seized servers, where a wealth of criminal transactions is often stored.

Scientific insights

In order to find an answer to these questions, Delft University of Technology and FIOD have drawn up a joint research agenda working towards evidence-based financial cybercrime policing. As a pilot, students at the FIOD – and in particular FACT – worked with data from an underground market, namely 'Hansa Market'. With this data, it was possible to reconstruct the complete administration of the market. Under supervision of senior scientists from Delft University of Technology, the students developed a method to accurately calculate the turnover of facilitators. This way, the FIOD can seize criminal assets of sellers on these markets in a scientifically substantiated way.

A second method helps to identify central players in these markets, which contributes to the effective and efficient attributing of facilitators – think of sellers of stolen credit card data, for example. As an extension of this research, students will be working on a crime script analysis that automatically maps the money laundering techniques of facilitators on Telegram, an encrypted communication application. Recently, another graduate – working with the same market data – unraveled the security practices of these facilitators so that potential vulnerabilities in their security can be made visible. But above all, this provides a better picture of the business and security trade-offs that these sellers make.

Research program 2021-2024
The current collaboration is characterized by short-cycle projects – where research can be done opportunistically, provided that both Delft University of Technology and the FIOD can organize a clearly defined assignment and adequate supervision of students. Although this approach is already bearing fruit, and the first results in the scientific community and policing practice are finding its way, the downside of this approach is also becoming clear. Students have to be trained – which requires repetitive investments for all parties – and that makes short-cycle research often exploratory in nature. The gap that arises here is that of being able to build on previous results and to conduct longitudinal, in-depth research. Overcoming this gap brings the focus of the research program from unraveling phenomena alone, to fully understanding and intervening effectively on these phenomena.

By creating positions for PhD students, this new focus is given substance in the research program. Under supervision of senior faculty of Delft University of Technology and under the guidance of experts from the FIOD, these researchers can exclusively focus on in-depth, innovative research into effective and efficient actions against professional facilitators in the financial cybercrime ecosystem. The explicit intention is also to leave room for opportunistic, short-cycle projects on which graduate students can continue to work. This way, the research program brings together the best of both worlds. Multi-year, in-depth research supplemented with short-cycle, opportunistic and data-driven research projects. As the scientific supervision of both processes is handled by the same principal investigator (PI), synergy between the two can be optimally and structurally utilized.

Guiding principles
This project works towards a shared goal: evidence-based policing of financial cybercrime. Here, a distinction can be made in roles and tasks. First, conducting scientific research for the purpose of policing. Second, the investigation process itself. In this project, Delft University of Technology focuses solely on the first: conducting independent scientific research for the purpose of policing. The investigation process itself is a task that the FIOD carries out independently and Delft University of Technology has no prior knowledge of, or influence on. Vice versa, the FIOD has no say in how and what Delft University of Technology investigates and how it reports their findings.

The collaboration therefore includes the following activities at Delft University of Technology:

1. intensive supervision of (PhD) students,
2. conducting independent scientific research into themes or phenomena relevant to the FIOD / FACT,
3. dissemination of knowledge, for example by means of a workshop, etc.
4. giving ad-hoc (policy) advice.

Anti-Money Laundering efforts in The Netherlands –
Part 3 '*Regulation of Cryptocurrency in the Netherlands*
Prepared by dr. R.S. van Wegberg, Delft University of Technology, the Netherlands[1]

Background

Nowadays, so-called virtual currencies play an increasingly prominent role in the criminal, underground economy. Of all these virtual alternatives to traditional banking, cryptocurrencies in particular stand out. Recent threat reports suggest that criminals are increasingly using cryptocurrencies to divert criminal profits. Bitcoins are a popular form of payment among criminals. Europol even reports that bitcoin is used in more than 40% of all identified criminal payments in cybercrime investigations. Virtual currencies therefore can be seen as an important enabler of cybercrimes. The main reason for their popularity is that they are easy to use and relatively anonymous. Steadily, virtual currencies have also proven to be a vital part of criminal business processes. For example, ransomware victims are forced to exchange the ransom from fiat currency to bitcoin and transfer this amount to a specific bitcoin address provided by the criminals.

The prominent role of cryptocurrencies in illegitimate business, also infused new forms of money laundering. Between 2004 and 2016 the Dutch Police, in several State of Crime reports, identified a sharp increase in the adoption of virtual currencies in criminal offenses (Soudijn, 2019). Here, virtual currencies are a digital representation of value which is not backed by a central legal authority, such as a central bank. A currency exchange provider, delivers a service in which fiat currency can be converted to virtual currencies or vice versa. Therefore, they form a gateway between the traditional financial and virtual currency ecosystem.

Last year, the European Union's 5th Anti-Money Laundering Directive –
AMLD5 – which aims to regulate the use of virtual currencies as a tool for money laundering came into force. The Netherlands has implemented this directive swiftly in national legislation. The directive entails a duty for all exchange providers to register at a national authority. In order to obtain this registration, companies have to prove that they perform customer due diligence and monitor and track transactions continuously. Moreover, companies are obliged to notify authorities when suspicious transactions take place.

Legislation
First, we report in-depth on the development of legislation related to virtual currencies and money laundering in the European Union and the Netherlands. To improve readability, Figure 1 shows the timeline of the implementation of several Anti-Money Laundering Directives imposed by the European Union.

Today, the European legislation consists of six Anti-Money Laundering Directives. The first directive exclusively focussed on money laundering of drug profits. The 2nd Anti-Money Laundering Directive extended the illegal acts and professions subject to this legislation. Only the 3rd Anti-Money Laundering Directive made a start in focussing on the financing of terrorism as well. In 2015 renewed interest sparked adjustments to counter money laundering and terrorism financing effectively. The fourth Anti-Money Laundering Directive (2015/849) was introduced in June 2015 with a requirement that it be implemented in national legislation by June 2017. The goal of this revision to the third Anti-Money Laundering Directive was to strengthen regulation with regard to

[1] This part of the report was drafted with the much appreciated assistance of Cecile Volten.

customer identification. Moreover, information on the Ultimate Beneficial Owner (UBO) had to be registered in a central registry. Furthermore, the European Commission aimed to implement sector risk assessments to increase awareness of money laundering and terrorism financing risks. Two other key issues AMLD4 tried to address were a) establishing a course of action for treatment of countries outside the union, by setting up a list of high-risk countries and b) increasing the cooperation between Financial Intelligence Units (FIUs) by enhanced opportunities to exchange information. Next to the AMLD4 implementation, the Regulation Traceability of Money Transfers (2015/847) was introduced. This regulation obligated payment service providers to store names and account numbers of transactions and check the correctness of the information obtained in order to facilitate AML efforts.

In 2018, a revision to AMLD4 was introduced. The fifth Anti-Money Laundering Directive (2018/843) had to be implemented by member states by January 2020. The Directive entailed that exchange services, providing the service to exchange fiat currency to virtual currency and vice versa, and custodian wallet providers are also obliged to report suspicious transactions. Moreover, these entities have to be registered at a national authority. The directive included a definition of virtual currencies and stated that customer due diligence should not only be performed on new but also on existing customers.

At the end of 2018 the 6th AMLD was introduced, which extended the list of illegal acts and specified sanctions which are deemed effective, deterrent and proportionate. The directive had to be implemented by December 2020.

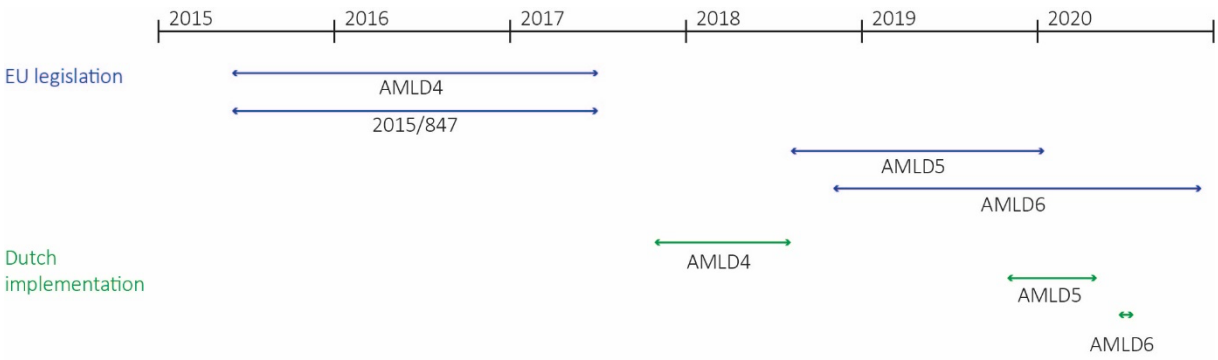

Figure 1 – Timeline of the implementation of the EU Anti-Money Laundering Directives in the Netherlands

At the time of the Dutch implementation of AMLD4, most debate concentrated on the Ultimate Beneficial Ownership registry. Only during the last stage of the implementation process did some politicians for the first time begin referring to and talking about bitcoin as a means of payment and the possible role of the currency in money laundering. At the time, new legislation was in the European Commission pipeline, but the AMLD4 did not yet cover virtual currencies.

In July 2019 the Dutch implementation of the 5th Anti-Money Laundering Directive started – this implementation altered the Wwft significantly. There were three reasons behind the implementation of AMLD5, namely a) the emergence of technology-driven services as alternatives to financial systems that were outside the scope of current legislation, b) the increasing interdependence of organized crime and terrorism threatening the security of the Union and c) the desirability of better cooperation between competent authorities of Member States. The directive also ensures that custodian wallet providers – i.e., a provider of a wallet service that can control

the virtual currency on behalf of the user – are subjected to legislation. Next, customer due diligence needs to be performed – which entails identifying the customers' identity based on legal documents or information from an independent source. Moreover, the relation between company and client needs to be assessed continuously and transactions need to be monitored closely. For all parties operating in countries outside of the EU, without a legal base inside the EU, there is a prohibition to offer services with virtual currencies in the Netherlands.

In the Dutch implementation of AMLD5, parliament desired a licensing, instead of a registration system. However, the Council of State, the prime legal advisory organ of government, advised against this as it considered this to be disproportionate. Thus, in the end, exchanges and wallet providers only needed to register at the Dutch Central Bank (DNB) – which also serves as the supervisor. The DNB can decline a registration request on three grounds: a) supplying incorrect data, b) supplying incomplete data or c) when the people or organizational unit in charge of day-to-day operations are deemed not reliable or trustworthy. After the implementation of AMLD5, all Dutch currency exchanges had up to six months to 'obtain' their registration. The providers of exchange services or custodian wallets have to set-up a user profile of their customer and based on this profile continuously assess the risk of a transaction by identifying whether the transaction is different from the expected profile. This way customer due diligence should be performed.

On the 23rd of March 2021 a court case was held between Bitonic and the Dutch Central Bank (DNB). Bitonic is a large Dutch currency exchange provider, which promises to instantly buy and sell bitcoin to its customers wallets. Bitonic argued that the Dutch Central Bank – as supervisor in the virtual currency ecosystem – applied rules that were too strict and not in line with the fifth Anti-Money Laundering Directive of the European Union. In its preliminary ruling, the court acknowledged Bitonic's objections and doubts about the registration procedure and the legality of the wallet verification requirement set by DNB. Although the court did not immediately suspend the wallet verification requirement, DNB is obliged to take a decision on Bitonic's objection within six weeks – before May 4th 2021.

Assessment of the strengths and weaknesses regulating virtual currencies

As virtual currencies pose a risk of money laundering, regulations have been put in place to limit these risks. Nonetheless, regulations fall short due to a lack of foresight by those creating the regulation leading to a legal grey area (Bryans, 2014). Böhme et al. (2015) identified four key intermediaries which can be subjected to regulation in the virtual currency ecosystem, namely: a) currency exchanges, b) digital wallet providers, c) mixers and d) mining pools. On top of these four intermediaries, Möser & Narayanan (2019) proposed to establish a blacklist to which coins can be checked in order to more easily detect illicit transactions and assist compliance to regulation. As the virtual currency system was not created against the backdrop of potential regulation, later on an idea was introduced of a three-tier regulatory framework consisting of self-regulation (Fletcher et al., 2021). Although these and other propositions for (self) regulation were made, the European Union decided to apply strict regulations solely to cryptocurrency exchanges, as anyone willing to exchange virtual to the fiat currencies or vice versa has to pass this portal. Following this logic, exchanges are deemed 'exploitable', regulatory chokepoints in the virtual currency economy (Meiklejohn et al., 2016; Stokes, 2012).

Next, we identify barriers for regulation of the virtual currency system. First, a definitional challenge is apparent. Some countries consider virtual currencies to be an asset, others a commodity or a currency. Moreover, the system lacks a governance structure other than its

underlying software which has several implications for the functioning of the system (Böhme et al., 2015). Therefore, there is no obligation from the system for user verification which checks users' identities and cross-checks them with watch-lists or embargoed countries. As there is limited information on identities, but perfect knowledge on transactions in the virtual currency system (Möser, 2013), this poses implications to the AML regime since all regimes were based on knowing your customer (KYC) (Campbell-Verduyn, 2017; Tu, 2015).

New technologies initiate a novel governance response which often leads to constriction in the adoption of technology (Campbell-Verduyn, 2017). In regulatory dialectic, policy makers draft reactive regulations (Dupuis, 2020). Therefore, several shortcomings of the regulation can be noted. First, the regulation does not apply to all trading platforms (De Vido, 2020; Dupuis & Gleason, 2020) since much trade is performed outside the centralized currency exchanges. Also, verified entities can be outdated and there is a challenge regarding the territoriality of the legislation (De Vido, 2019).

Not only were concerns voiced as to the effectiveness of the regulation, concerns were also voiced on the mandatory adoption of tools to detect suspicious transactions by currency exchanges (Möser & Narayanan, 2019). This could lead to privacy issues for all virtual currency users. Moreover, individual users making payments outside of these services do not have access to those compliance tools to perform customer due diligence and will thus have a heightened chance of acquiring illicit coins.

References

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, *29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Campbell-Verduyn, M. (2017). Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance. In *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*. https://doi.org/10.4324/9781315211909

De Vido, S. (2019). The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive. *DPCE Online*, *1*(May), 59–76.

De Vido, S. (2020). Virtual Currencies: New Challenges to the Right to Privacy? An Assessment under the v AML Directive and the GDPR. *Global Jurist*, *20*(2), 1–14. https://doi.org/10.1515/gj-2019-0045

Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*, *ahead-of-p*(ahead-of-print). https://doi.org/10.1108/JFC-06-2020-0113

Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance*, *56*(January), 101387. https://doi.org/10.1016/j.ribaf.2021.101387

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A fistful of Bitcoins. *Communications of the ACM*, *59*(4), 86–93. https://doi.org/10.1145/2896384

Moser, M., Bohme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *ECrime Researchers Summit, ECrime*, 1–14. https://doi.org/10.1109/eCRS.2013.6805780

Soudijn, M. R. J. (2019). *Using Police Reports to Monitor Money Laundering Developments . Continuity and Change in 12 Years of Dutch Money Laundering Crime Pattern Analyses*. 83–97.

Stokes, R. (2012). *Information & Communications Technology Law Virtual money laundering: the case of Bitcoin and the Linden dollar*. https://doi.org/10.1080/13600834.2012.744225
The Blockchain Analysis Company. (n.d.). Chainalysis. Retrieved March 22, 2021, from https://www.chainalysis.com/

Tropina, T. (2014). Fighting money laundering in the age of online banking, virtual currencies and internet gambling. *ERA Forum*, *15*(1), 69–84. https://doi.org/10.1007/s12027-014-0335-2

Tu, K. V., & Meredith, M. W. (2015). Rethinking virtual currency regulation in the bitcoin age. *Washington Law Review*, *90*(1), 271–347.