Fennoscandic comparison on KYC obligations of a virtual currency provider

Keskitalo, Kristian; Väyrynen, Jaakko

2023-07-04
EMERALD GROUP PUBLISHING LTD
http://hdl.handle.net/10138/567471
Keskitalo, K & Väyrynen, J 2023, 'Fennoscandic comparison on KYC obligations of a virtual currency provider', Journal of Money Laundering Control, vol. 26, no. 7, pp. 167-180. https://doi.org/10.1108/JMLC-12-2022-0168

Fennoscandic comparison on KYC obligations of a virtual currency provider

Kristian Keskitalo
Faculty of Law, University of Helsinki – City Centre Campus, Helsinki, Finland, and

Jaakko Väyrynen
Settle Group AS, Oslo, Norway

Abstract

Purpose – This paper aims to analyse the virtual currency regulation especially in Finland, Sweden and Norway. Different member states had a bit differently incorporated regulation of AMLD5. Finland has gone the furthest in regulation and even issuers of virtual currency are under the Finnish regulation.

Design/methodology/approach – In one hand, the study approach is legal dogmatics, but in other hand it is comparative legal research. Both approaches can be found in this paper.

Findings – The EEA is going from a more fragmented regulatory landscape based on 5th Anti-Money Laundering Directive to a more uniform regulatory approach provided by a legislative package that regulates crypto assets more broadly, coupled with an overhaul of the anti-money laundering rules, bringing them into a single European rulebook. Finland has taken a step further in this matter. Therefore, it would be reasonable for the AMLD5 scope to be expanded in this respect. It is a welcome development that the regulation will be unified and that investor protection will be better taken into account in the future as well.

Originality/value – This paper gives a picture of what kind of challenges is there in Fennoscandic in terms of money laundering regulation of virtual currencies. On the other hand, this paper brings into the discussion the rather clever solutions of Fennoscandic (especially Finland) regarding money laundering of virtual currencies.

Keywords KYC, Cryptocurrency, Know your customer

Paper type Research paper

1. Introduction

Virtual currencies [1] are no longer a niche sparking the interest of only the most hardcore tech enthusiasts, but have swiftly gained popularity amongst the general public, leading to the need to mitigate the ambiguities and risks associated with virtual currencies through legislation. In some European Union (EU) (or European Economic Area) member states [2], the regulatory efforts have been initiated by extending the scope of current anti-money laundering (AML) legislation to also cover doing business with virtual currencies more widely – this development is not a fragmented effort of separate member states but the

Journal of Money Laundering Control
Vol. 26 No. 7, 2023
pp. 167-180
Emerald Publishing Limited
1368-5201
DOI 10.1108/JMLC-12-2022-0168

implementation of the 5th Anti-Money Laundering Directive (Directive [EU] 2018/843; hereinafter "AMLD5") enacted by the EU to make virtual currencies part of money laundering legislation. The reason for the regulation is that most crypto activities have fallen outside any previous regulation, causing virtual currencies to become a tool for illegal transactions. However, virtual currencies still have not risen to the level of the perceived risk they are often attributed, and only a small share of completed virtual currency transactions have been demonstrably connected to criminal activity (Chainalysis, 2022), which has so far been less than the respective share for traditional finance in absolute and relative terms (United Nations Office on Drugs and Crime, 2022). This raises the question: Are virtual currencies in need of specialised AML efforts, or should the focus be kept on traditional finance, which is the main avenue for laundering illegally obtained funds? Also, the claims that the anonymous nature of virtual currencies poses a considerable money laundering and terrorism financing risk are often overstated due to the simple fact that most virtual currencies are not in fact anonymous [3] (The Finnish Government, 2018). Against this backdrop, this article will later discuss the adequacy and proportionality of the current regulatory environment and proposed changes to the AML framework within the European Economic Area.

Although based on the AMLD5, the national legislative acts implementing the AMLD5 are somewhat fragmented and, as will be shown, some member states have gone further than what is required in the AMLD5 on the basis of public policy by extending the scope of regulated virtual currency (asset) service providers or regulated transaction types, with Finland as our primary specimen (The Finnish Government, 2018). These peculiarities in the adoption of AMLD5 by some member states will be tied to the analysis of the current regulatory environment, how these peculiarities have functioned in practice, and whether they ought to be more widely adopted, or if they are potentially already covered in the next AML legislation package proposed by the EU. The article specifically deals with the regulation of Finland, Sweden and Norway. The regulation in the Nordic countries has traditionally been considered quite uniform, and because of this, the examination of the regulation in those countries is particularly interesting. In addition, in Finland, AMLD5 has been enacted as a separate act on virtual currency providers, where the regulation goes beyond what AMLD5 requires in quite a few points. The main focus of the analysis shall be on the scope of virtual currency (asset) service providers, and the types of assets and transactions covered by "Know Your Customer" (KYC) obligations under the current regulations.

2. Current regulatory framework

2.1 European anti-money laundering legislation

The AML legislation in the EU has been ever evolving, and in their effort to curb the use of new technologies for illicit purposes and mitigate the risks to the integrity of the financial system. The introduction of virtual currencies and virtual currency providers under the scope of AMLD5 underlines the growing importance of this emerging sector in finance and the need for its urgent regulation with its aim to increase the services providers' transparency and accountability protecting the financial system as a whole from being used for criminal purposes. Maybe the most significant introduction amending the 4th Anti-Money Laundering Directive can be found in article 1(1)(c), as AMLD5 adds "providers engaged in exchange services between virtual currencies and fiat currencies" (hereinafter "crypto exchanges") and "custodian wallet providers" to the list of obliged entities under the EU's AML rules, and in article 1(2)(d) it further defines a virtual currency as:

> [. . .] a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically

and a custodian wallet provider as "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies".

Hence, AMLD5 defines virtual currencies very broadly, as in practice many non-virtual currencies could potentially fulfil the requirements of the definition. However, the directive goes on to negatively define virtual currencies in AMLD5 recital 10 by excluding, e.g. electronic money and in-game currencies from the scope and thus limiting the definition. This exclusion is significant to eliminate overlap with entities regulated to a different extend (e-money) and exclude non-material currencies for illicit purposes (in-game).

More interestingly for the purposes of this article, we are looking at the scope of obliged entities in the virtual currency industry, which could be argued to be somewhat narrow; the obliged entities consist of an on/off-ramp between virtual and fiat currencies (crypto exchanges) and hosted storage of virtual currencies (custodian wallet providers), further narrowed by the directive definition of custodian wallet providers, limiting them to services that "safeguard private cryptographic keys on behalf of [their] customers", which could be argued to exclude certain types of nominee holding services (discussed later) from the directive's scope. To this date, there have been no preliminary cases in the Court of Justice of the EU on these definitions, while the limited nature of the definitions has prompted action from the member states and national transpositions have been worded differently to extend the scope of service providers falling under the category of obliged entities.

The definitions are understandably broad, as to not exclude any prominent virtual currencies and service providers from the scope of regulation as anti-money laundering regulations tend to lag behind the methods used to cover the origins of illicit gains. Hence, for regulation to be effective, the definitions ought to be sufficiently broad without being too ambiguous and unclear. As demonstrated below by the transpositions in the specimen countries, not all national legislators agree on the scope of AMLD5's definitions and have sought to either clarify or broaden the definitions in their national laws. However, when regulation on EU level is not seen as providing sufficient breadth and clarity in its scope, it causes regulatory fragmentation and inefficiencies in the internal market. This begs the question: Is directive-based regulation enough to balance efficient prevention of criminal flow of funds and regulatory arbitrage against efficient facilitation of legal flows of funds and commerce within the bloc, or is fragmentation mandating a more harmonised approach?

2.2 National anti-money laundering legislation comparison

2.2.1 Finland. The clearest departure from the definitions offered by AMLD5 was adopted in Finland; this is one example of a state going beyond the scope of what is required by AMLD5 introducing a broader scope, which was stated in the Draft Bill proposed by the government (The Finnish Government, 2018). The enacted law on virtual currency providers (*Laki Virtuaalivaluuttojen Tarjoajista 572/2019;* hereinafter "VVTL") has some unique features in comparison to the other specimens in this article, and will be examined more closely.

One unique feature of VVTL is that it extends the scope of obliged entities to issuers of virtual currencies ("virtuaalivaluutan liikkeellelaskija"; which, as a term, is arguably derived from its relatives in traditional finance, such as an issuer of electronic money); hence, VVTL obliging these issuers to know their customers under its section 13. Who then is a customer of an issuer of virtual currencies, and how far-reaching is this obligation down

the chain of holders of the issued currency? To date, there has been no jurisprudence of the court on this point of law, and legal literature has been silent on the matter. The question, however, is significant to industry players and warrants a closer look.

One potential answer to the question of interpretation has been brought up by some industry players, whose view is that the KYC obligation of a virtual currency issuer exists from the first transfer of the currency to a party who is not the issuer, up until the currency is held by anyone other than the issuer [4], which implies that anyone holding that virtual currency, even after multiple private transactions, would be a customer of the issuer and hence be identified by the issuer. If this view were to be accepted, it would raise more questions than it would answer. To backtrack and answer the question satisfactorily, we need to look at what is meant by "customer", "issuer", "provider" and "business" for the purposes of VVTL, to determine its actual scope.

Section 2 of VVTL lists the new obliged entities that are deemed virtual currency providers as "virtual currency issuers, virtual currency exchange services or marketplaces, or wallet service providers", hence making the category of obliged entities broader than what is required by AMLD5 by not only adding issuers but virtual currency marketplaces as well. *Prima facie*, it appears that VVTL follows the same logic as AMLD5 by excluding cold storage wallets [5] (as long as they are used by non-service providers, as VVTL only applies to service providers) and hence purely private transactions between persons (see Figure 1).

2.2.1.1 Issuer. VVTL section 2, paragraph 3, defines "issuer" only very briefly as "a natural or legal person that issues virtual currency". This circularly defined term may be the origin of confusion amongst industry players considering the wide variety of virtual currencies and how they are created and "issued"; placing them all under an umbrella term causes problems in the interpretation of the law. Hence, in the interests of clarity and legal certainty, a more detailed definition would be welcome, which shall be evidenced below by illustrating the differences between various types of virtual currencies (or assets).

As with many of the most prominent virtual currencies that are purely decentralised, such as bitcoin, there is no single entity that "issues virtual currencies to customers". Instead more of the same currency is created by independent nodes based on the rules of the blockchain and its consensus algorithms, thus making it impossible to identify an issuer (Keskitalo, 2022a, 2022b). This fact is also stated in the Bill, which makes the Act's final drafting seem rushed and incomplete. However, the Bill goes on to consider that issuers ought to fall within the scope of the Act due to the risks posed by virtual currencies, and later brings up Initial Coin Offerings (ICOs), where "in connection with the issuer describes the features and uses of the virtual currency, and the terms for the offering" (The Finnish Government, 2018). This implies that the reason for the inclusion of virtual currency issuers is based on mitigating fraud risk and enhancing investor protection,

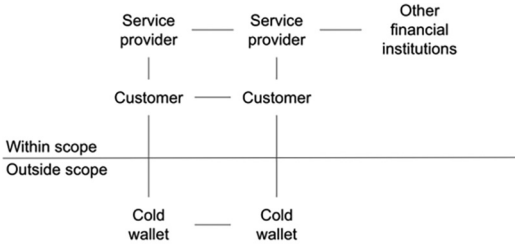


Figure 1.
KYC obligations and transactions within the scope of AMLD5

Source: Keskitalo and Väyrynen (2022)

rather than their inherent AML risks. Hence, an issuer must mean an identifiable entity that conducts business by issuing virtual currencies to the public, thus limiting the definition to some extent.

On the contrary, centralised virtual currencies, or their blockchains, bring a new perspective to the interpretation of the term "issuer", when there is an identifiable entity or entities controlling the operation of the blockchain and its consensus algorithms, as in the case of Ripple (XRP), which is a virtual currency based on a closed and centralised blockchain (Chase and MacBrough, 2018). Once identifiable, it could be argued that the community or entity that has created or administers the blockchain could be deemed the issuer. But could a holder of XRP be deemed a customer of Ripple? According to VVTL and its preliminary drafts, yes, which would be in line with the Proposal for a Regulation of the European Parliament and of the Council on the cryptocurrency market and amending Directive (EU) 2019/1937, COM (2020) 593 final, article. 3, paragraphs 6 and 18 (discussed later), which states that the issuer's management body is the actor that exercises decision-making authority in the community. This would support our previous proposal that VVTL aims to regulate issuers with centralised systems that have an identifiable beneficiary [6]. Interpreted from this angle, virtual currencies with decentralised systems *may* also have an issuer if the origins of the virtual currency can be traced to an identifiable entity or entities, making the assessment of an "issuer" a case-by-case exercise as opposed to a clear-cut rule.

2.2.1.2 Exchange services. In addition to what is stated in Section 1 of VVTL, Paragraph 4 of Section 2 also requires that any exchange activity be performed as a business or professional activity for it to fall within the scope of the Act. The following virtual currency exchange operations are considered exchange services:

- the virtual currency is exchanged for a legal means of payment or another virtual currency;
- it is exchanged as a service for another commodity or vice versa; or
- the entity maintains a marketplace where the service from the previous points can be performed.

As stated above, this goes beyond the required level of AMLD5 and brings marketplaces and crypto-to-crypto exchanges within the scope of regulation, which is easily justified in the interests of combating AML and terrorism financing due to its proportionality (The Finnish Government, 2018). When the matter is mirrored even more broadly with the purpose of preventing money laundering and terrorist financing, it is also quite justified to include exchanging virtual currency for commodities as a business or professional activity within the scope [7]. If the categorical exchange service aimed at commodities had been left out of the regulation, it would be more challenging or even impossible to target money laundering and terrorist financing prevention measures or obligations at the parties engaged in the business in question. As far as service provision and marketplaces are concerned, there would seem to be no major questions of interpretation, and the provision seems quite clear in this regard.

However, the exchange of virtual currency for goods raises the question of whether a business transaction in which virtual currency is received as payment for a service or goods can be considered an exchange service according to point (ii) in the previous paragraph. The Bill only gives an example of virtual currency being exchanged for a valuable commodity such as gold (The Finnish Government, 2018). But due to VVTL only applying to exchange services that are conducted as a (virtual currency) business or professional activity, it could be argued that if an entity's business is something other than providing those exchange

services, e.g. a barber accepting virtual currency as payment, it would not be considered an exchange service provider for the purposes of VVTL. However, it could be that an entity's actual business should be considered on a case-by-case basis; the interpretation could change in fringe cases if the barber accepted only virtual currencies and not any conventional payment methods, such as cash, card or mobile payments.

2.2.1.3 Wallet services. For the purposes of VVTL, a wallet service provider means an entity that holds virtual currency on behalf of another or offers its transfer or storage. AMLD5 expressly stipulates in article 1(2)(d) that a wallet service refers to an entity that "offers services to secure private encryption keys on behalf of its customers in order to hold, store and transfer virtual currencies", making the AMLD5 definition narrower than its VVTL counterpart. This definition of VVTL can be considered justified, so that service providers who do not keep the customer's encryption keys, but buy virtual currency in their own name, store it on behalf of the customer as nominees (so-called "off-chain" or outside the blockchain trading and storage arrangement), and manage these stored virtual currencies on behalf of the customer in a prescribed manner, are not left outside the scope of the Act; the service provider could combine orders from several clients, thus it would be practically impossible to allocate the private encryption key belonging to an individual client. Here, the service provider does not explicitly separate or assign virtual currencies in such a way that it can be determined from this common asset mass which virtual currencies are assigned to which client. On the one hand, it may also be possible that the virtual currencies are at one address according to the public key and thus behind one private encryption key, which is why the private encryption key cannot be assigned to one principal. Although *de facto* exchange services, these service types would fall outside AMLD5 but be included in the scope of VVTL due to its omission of the encryption key requirement.

2.2.1.4 Business or professional activity. VVTL's scope encompasses only virtual currency providers that operate as businesses; hence, it is imperative to examine what is considered "business".

According to the Bill, whether the provider is a business is considered on a case-by-case basis; there are no monetary limits, and the Bill states that hobby activities would be excluded from the scope of VVTL, even if the activity is significant in terms of monetary value. Without further definition by the draftsman in VVTL or other AML legislation, we are again left with a vague term that causes problems in interpretation. Because the content of business and professional activities has not been defined in greater detail, some help for interpretation can be sought from tax law, where the boundaries of a business are drawn frequently. However, it must be emphasised that the definition is for the purposes of a directive aimed at preventing money laundering and terrorism financing, and thus might require a different approach from tax law, in which the evaluation of the business is influenced, among other things, by whether the service is widely offered to the public and whether the activity has a profit-making purpose [8]. In addition, operating in the form of a company may indicate that the activity has a business purpose, even though operating in the form of a company does not categorically mean that the activity is conducted as a business, but may only be an ancillary activity. For example, it may be possible that a cooperative produces a service only for a small group of associated people, in which case the business criterion may not be met.

In connection with the virtual currency issuer, the Bill points out that risks have been detected in ICOs with regard to virtual currency, i.e. in crowdfunding, where the virtual currency is launched for the first time by the developing *community* (The Finnish Government, 2018). If an entity launches a virtual currency, is it automatically considered a business falling within the scope of VVTL? If an entity is engaged in other business

activities, should the ICO be considered such an essential part of the main business, albeit as an ancillary part of it, so that the ICO could be interpreted as fulfilling the business criteria set for the issuer? In our view, the situation would be unambiguous, at least if the entity does not conduct business at all, but, for example, a public benefit activity, and to finance that activity the entity organises an ICO. In this case, the ICO would not exceed the business criterion for the purposes of VVTL, unless the activities concerning the ICO are otherwise extensive. Categorically, however, an ICO could not be interpreted as a business according to VVTL, if it generally finances only other business than activities covered by VVTL.

2.2.1.5 Know your customer. Section 13 of the VVTL sets out the duty for the obliged entities to know their customers ("KYC"): the Financial Supervisory Authority can give more detailed instructions on the procedures to be followed in KYC and customer risk management, and with regards to KYC the Act on the Prevention and Investigation of Money Laundering and Terrorism Financing (444/2017) also applies. For the purposes of this article, we are interested in the definition of *customer* for the purposes of VVTL; the customer is not defined any further in the Bill nor elsewhere in current AML legislation. In previous drafts of the national laws regarding the prevention and investigation of money laundering and terrorist financing, the concept of customer has been stated as follows: "[a] customer means a natural person or legal entity to whom – [virtual currency provider] offers services or who requests or uses – [virtual currency provider's] services. Permanent customer relationship means a relationship of a permanent nature or a relationship that is assumed to become permanent at the time of contact. This kind of establishing a customer relationship can be, for example, opening an account, entering into a credit agreement, subscribing to a fund, entering into a securities brokerage or commission agreement". (The Finnish Government, 2008). In legal literature, Cox has tied the duty to know the customer, and thus indirectly the concept of the customer itself, to the financial relationship between the parties (*inter partes*) strongly (Cox, 2014).

When the concept of the customer is considered in connection with the purpose of AML regulation, the draft bills and what is presented in legal literature, it has a similar meaning to how it would be defined in a dictionary. Accordingly, all transactions involving the transfer of funds in a broad sense – such as a trade, contractual relationship or other exchange relationship with another party – should be concluded with a customer. Therefore, the obligation to know the customer as such begins even before the actual transaction and lasts throughout the customer relationship [9].

It is therefore the financial relationship between the issuer and the customer that is the decisive factor in determining who is a customer of an issuer. Arguably, any latter transferees subsequent to the initial transfer between the issuer and the first transferee would not fulfil the determining factor, as the financial relationship only exists between the first transferee (customer) and the latter transferee, and not the issuer. However, in some cases, the issuer *may* end up in a customer relationship with a later transferee, for example, in the case of some types of utility tokens: these utility tokens can function in a decentralised and open or closed blockchain, but serve a certain specific purpose in the ecosystem built around it. The utility tokens in question can be considered to return to the original issuer when a token is exchanged for possible goods or services produced by the issuer. In this case, the customer relationship with the holder of the token could be considered as being created in connection with the first and last transaction (see Figure 2): when the commodity token is initially issued (1.) and when it is redeemed (2.). In this case, the issuer's duty to know the customer could be limited only to these transactions, in which case other transactions fall outside the issuer's duty to know the customer.

2.2.1.6 Conclusion – Finland. Finland has decided to go beyond AMLD5 not only by enacting a separate Act (VVTL) on virtual currency providers as opposed to only extending the obliged entities list in the general AML legislation, but also by going beyond the scope of what is required by AMLD5. This is partially motivated by the need for further industry regulation in other fields of law as well, and not only AML; this arguably points to further European-level legislative efforts being long overdue, as including. e.g. issuers in AML legislation causes interpretational problems and, without further guidance from the regulators, leaves the industry hanging in an uncertain position. As virtual currencies raise fundamental questions not touched upon before, it is difficult to apply for interpretational help from other areas of law. In any case, as far as the issuer is concerned, VVTL is only rarely suitable, and it is rather an ICO-like fundraising or a so-called private virtual currency, for which the question may arise as to whether it is a virtual currency launched for business purposes. Similarly, the definition of the customer and the related obligation to know the customer largely return to the common-language meaning.

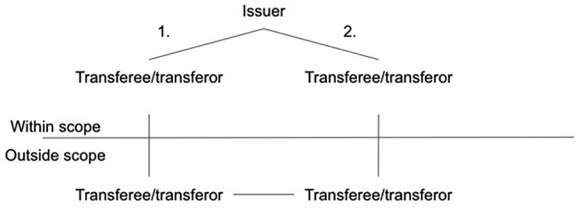
It can be argued that the view put forward by industry players, as to whether the obligation to know the customer could apply from the issuer of virtual currency all the way to those third parties to whom the customer of the issuer hands over the virtual currency, seems to be a rather far-fetched interpretation, which does not seem to be based on the purpose of the law, its preambles or other legal literature. One can also justifiably ask whether it has been necessary to regulate the issuer under AML legislation. ICOs could arguably be covered by VVTL because all entities that hand over virtual currency against fiat currency would be included in the broad definition of exchange services. Next, these peculiarities shall be contrasted with the practices of some other EU/EEA member states that have not been as aggressive in regulating virtual currency providers beyond the requirements of AMLD5.

2.2.2 Sweden. As opposed to Finland, the Swedish legislature has not enacted a separate act for virtual currency providers, but amended its existing financial and AML legislation in line with AMLD5; however, it also extended the scope beyond what is required by the directive, albeit to a lesser extent than its eastern neighbour.

Sweden lumps virtual currency providers together in Act (1996:1006) on currency exchange (Lag [1996:1006] om valutäväxling och annan finansiell verskell) with a category of "other financial activity" consisting of:

> [. . .] professional activity that consists of management of or trading in virtual currency or that mainly consists in carrying out one or more of the activities specified in chapter 7. Section 1 second paragraph 2, 3 and 5-12 of the Act (2004:297) on banking and financing operations [which includes e.g. granting and mediation of credit, receivables acquiring, and providing financial advice].

Hence, the provision of virtual currency services is equated with more traditional financial services, making the assessment of the actual scope of the act on various types of virtual



Source: Keskitalo and Väyrynen (2022)

Figure 2.
Issuer's KYC obligations

currency activities slightly easier. For example, the definition of who is a customer of a financial institution is clearly stated in the (Swedish) Anti-Money Laundering Act [Lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism; hereinafter "SAMLA"]; "[a] customer [is a] person who has entered into or is about to enter into a contractual relationship with such business operator as referred to in this Act". This definition seems to match our conclusion of what a customer is under VVTL.

However, some terms regarding virtual currency providers require further investigation: what is the scope of "professional activity" (yrkesmässig verksamhet), and "management of or trading in" (förvaltning av eller handel med)?

In the initial proposal for the implementation of the directive, it was put forward that only wallet providers need to be added as obliged entities, as exchange services between virtual currencies and fiat currencies would already be covered by existing legislation (Ministry of Finance, 2018). This was seen by the supervisory authority(Finansinspektionen) as inadequate to combat the money laundering and terrorism financing risks due to the existing main activity requirement, which ought to be omitted with regards to virtual currencies, and the exclusion of exchange services between virtual currencies, which ought to be included (The Swedish Financial Supervisory Authority, 2018). These changes proposed by the Swedish Financial Supervisory Authority were adopted in the final text. Although it does not explicitly mention exchange services between virtual currencies, trading virtual currencies (or virtual currency trading) arguably extends the scope of the Act in comparison to the initial proposal by including all trading activity, and further beyond the scope of AMLD5. Trading is not further defined in the same act or other related acts, hence its dictionary meaning of "buying or selling" could arguably be adopted, which would match the legislative intent of extending the scope to also include exchange services between virtual currencies.

"Management of", which in the final text replaced the term "wallet services" introduced in the initial proposal, has also not been defined further, and arguably again extends the scope of the obliged entities further than what is required in the directive. If given a dictionary meaning, the management of virtual currencies would also include nominee services, which are not covered by the definition given to custodian wallet services in the directive (Ministry of Finance, 2018). However, management arguably goes further than storing or holding, which is the usual function of wallet services. Management could be argued to include wealth management services in virtual currencies.

Professional activity, although also found elsewhere in SAMLA, has not been defined specifically in either AML or financial services legislation; hence, we are required to seek aid in interpretation from other fields of law. Again, as in the case of Finland, some help for defining professional activity could be found in the realm of tax law, where this question often arises regarding, e.g. VAT liability, highlighting the fact that AMLD5 still has an unclear scope until CJEU is presented with a case where these definitions are further considered.

2.2.3 Norway. Norway has approached the regulation of virtual currency providers with the lightest touch of the specimens examined here: the Norwegian Anti-Money Laundering Act [Lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven) (2018); hereinafter "NAMLA"] gives the government discretionary authority to regulate virtual currencies in the form of a regulation, which the government has done by adding a clause in the Anti-Money Laundering Regulation (Forskrift om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften); hereinafter "NAMLR") which transposes AMLD5's requirements by including custody services, which are defined word-for-word as in AMLD5, including the requirement of storage of private cryptographic keys on behalf of the customer, and exchange services, without limiting those to transactions between fiats

and virtual currencies, as is done in AMLD5. In a circular from the Financial Supervisory Authority (Finanstilsynet), exchange services are further defined to include:

> [. . .] trade or exchange a type of virtual currency for an official currency or vice versa [. . .]; exchange between different types of virtual currencies [. . .]; and facilitating trade and exchanges by connecting buyers and sellers, for example through a platform.

Norway has omitted the requirement of these activities to be done "as a business" or "as professional activity" which arguably extends the scope of application with regard to the nature of the service provision; according to s.1(3)(1) of NAMLR, all providers engaging in these activities must register with the Financial Supervisory Authority and are therefore obliged to follow the obligations under the NAMLA. This omission of a professional activity requirement seems to be intentional, as the position is further elaborated by the Financial Supervisory Authority:

> The service providers are covered by the regulations by virtue of the services they offer, regardless of how the service is organised. The registration obligation therefore also includes service providers who, for example, operate without being registered in the business register, operate via a private account, operate through platforms, or foreign providers who target the Norwegian market. It is the activity itself that is the basis for the registration obligation.

Taking away this ambiguity, the scope of NAMLR is extended as to the nature of how the services are organised, and the Norwegian legislative position is clear(er)-cut as to which entities have KYC obligations.

We will again need to look at the extent of that obligation by investigating who is a customer for the purposes of NAMLA. NAMLA does not define customer *per se*, but the KYC obligations centre around the establishment of a customer relationship, which would point to it being an economical and contractual relationship, making it the same as the definition in SAMLA. Note, however, that KYC obligations do extend outside customer relationships as well to one-time transactions where there is no customer relationship as long as certain monetary limits are reached or if an obliged entity suspects money laundering or terrorism financing.

2.3 Comparative conclusion

Our examples demonstrate three different approaches to the transposition of the directive into the national law: Norway mostly adopted the wording of the directive, Sweden expanded the scope by changing terminology and Finland expanded the scope even further by introducing a new type of service provider to be regulated. As typical for a regulatory landscape based on a directive, there is clear fragmentation between the member states, which affects the efficacy of the internal market in the virtual currency industry, especially when passporting solutions are taken off the table by divergence in national laws causing supervision of virtual currency providers to be non-comparable, and hence non-passportable, in many cases.

As previously mentioned, some member states have extended the scope of obliged entities in AML regulations due to the lack of regulation of virtual currency providers elsewhere in financial regulations, which implies some urgency in regulating the industry more broadly, and not only by reining in bad actors with AML rules that are not necessarily well-suited to achieving other goals, e.g. preventing fraud, and may only cause difficulties in interpreting legislation, as in the case of the term issuer in Finnish law. This lack of more appropriate regulation has clearly not been ignored by the EU Commission, as they have proposed a new legislative package regulating virtual currency providers more broadly; in

the next part, we will take a look at how the proposed regulatory changes on the EU level might clarify the issues raised in this article.

3. A look into the future

The EU Commission has brought forward a proposal for a new legislative package on virtual currencies. In addition to placing most AML rules in a regulation to uniformise the regulatory landscape (COM/2021/420 final), the proposed package would also regulate the virtual currency more extensively and rigorously, addressing the concerns that the member states have signalled through their varying implementations of AMLD5, which have arguably encroached on the field of investor protection. Markets in Crypto Assets Regulation (COM (2020) 593 final; hereinafter "MiCA") shall act as the primary source of terminology for virtual currencies and other virtual currency (assets): refreshed terminology that is better suited to cover various types of industry players.

MiCA's definition of Crypto Asset Service Providers (hereinafter "CASP") as "any person whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis" and a crypto-asset service for the purposes of the regulation:

means any of the services and activities listed below relating to any crypto-asset:

- the custody and administration of crypto-assets on behalf of third parties;
- the operation of a trading platform for crypto-assets;
- the exchange of crypto-assets for fiat currency that is legal tender;
- the exchange of crypto-assets for other crypto-assets;
- the execution of orders for crypto-assets on behalf of third parties;
- placing of crypto-assets;
- the reception and transmission of orders for crypto-assets on behalf of third parties; and
- providing advice on crypto-assets.

The service providers regulated by MiCA also fall within the ambit of AML rules. Notwithstanding the less open-ended definitions in comparison to AMLD5 and its implementing acts, the scope of obliged entities has been broadened from wallet and exchange services to cover a larger field of industry actors, including issuers, trading platforms and administration of crypto assets, which were some of the actors regulated by individual countries (see e.g. Finland and Sweden) under current laws. Also, MiCA makes it more explicit that those services need to be provided in the course of one's business or occupation and on a professional basis to be considered a CASP. This can be contrasted with Norway's current position, which also includes non-professional activity.

The scope of the KYC obligations of these obliged entities is expanded even further by the proposed application of the Travel Rule (COM/2021/422 final) to any unhosted (cold) wallets if a transaction reaches the limit of €1,000, at which point a service provider would be required to validate that the cold wallet is in possession of the person who is named as the sender or recipient of the transaction. Of course, this could apply only for the service providers if someone can even be identified for this purpose. Although good for preventing money laundering, this measure may present a privacy problem due to the pseudonymous nature of most crypto assets, as when a cold wallet is identified, not only the transaction that falls within the travel rule is known, but other transactions made from that cold wallet can then also be traced to a person on the basis of the travel rule.

4. Conclusion

The developments in crypto asset regulation are long overdue, as can be seen in the latest news regarding crypto exchange FTX's bankruptcy due to a lack of internal safeguards despite holding billions in customer funds (The Guardian, 2022). However, the problems within the crypto industry have not necessarily been in the sphere of AML (when compared to traditional finance, see p. 1) but rather the lack of investor protection, as in the case of FTX. This begs the question of whether starting crypto regulatory efforts from introducing crypto asset service providers in AMLD5 was the most efficient way to weed out rogue actors in the industry or curb money laundering more widely, or if the efforts should still be mostly aimed at uprooting the inherent AML problems within traditional finance, considering that the amount laundered through traditional finance is still a hundred-fold that in crypto. There may be an advantage in regulating an industry early to avoid playing catch-up with rogue actors later down the road, as has arguably happened with traditional finance, and crypto assets do have the potential to become a more significant medium for money laundering and terrorism financing due to their effortless global reach.

As shown above, the EEA is going from a more fragmented regulatory landscape based on AMLD5 to a more uniform regulatory approach provided by a legislative package that regulates crypto assets more broadly, coupled with an overhaul of the AML rules, bringing them into a single European rulebook. However, Finnish regulation can still be seen to have a significant advantage in relation to money laundering. Just as the ineffectiveness of the AMLD5 regulation has been criticised in the legal literature before, Finland has taken a step further in this matter. Therefore, it would be reasonable for the AMLD5 scope to be expanded in this respect. It is a welcome development that the regulation will be unified, and that investor protection will be better taken into account in the future as well.

It is quite justified to include virtual currencies as a target of money laundering regulations because, even though cash has its own fundamental problem and other electronic payment methods are generally covered by AML regulations, virtual currencies have the potential to create a separate black market if left unregulated. Financial criminals could use virtual currencies for illicit activities, and without proper regulation, the funds could move out of the scope of supervision. On the contrary, if transactions between virtual currency and cash were only within the scope of regulation, as they are based on AMLD5, then a significant part of money laundering could be covered. However, it is important to note that non-regulated money laundering cannot be ruled out, such as transactions made directly with virtual currencies or exchanging them for goods (low value). The challenges of money laundering are rooted in mining, which is often significantly capital intensive. Regarding the regulation of money laundering, there is a risk that virtual currencies will be over-regulated, which may stifle the entire innovative business related to blockchain technology in Europe.

However, the article shows that there are significant differences in the regulation of virtual currency between countries. This is not desirable, because ultimately this enables regulation "shopping". Ultimately, a EU regulation on money laundering regarding virtual currencies would be appropriate. This would often prevent complex situations for transnational operators, but it would also eliminate the problem in the EU area that companies whose business is focused on virtual currencies concentrate in a certain target country in pursuit of lighter regulation.

Notes

1. Instead of virtual currency, it would be more appropriate to use virtual assets as the overarching concept, for example, because they also include instruments designed for many other purposes than only for use as a means of payment or investment. However, due to the terminology used in the legislation, the term "virtual currency" is used in this article (Keskitalo, 2022).
2. In this article, the current regulation regarding virtual currency in Finland, Norway and Sweden are considered.
3. Transactions made with virtual currency are generally pseudonymous, and thus so-called cash offers the transferor of funds significantly higher anonymity than virtual currencies. However, it is more challenging to transfer large amounts of cash internationally than by performing an electronic funds transfer (Keskitalo, 2022a, 2022b).
4. View taken by e.g. Martin Wichmann 15/09/2021 at Fyfy's pre-ICO panel, the future of payment and digitalisation (FYFY, 2021).
5. A cold wallet usually refers to a hardware wallet or a so-called paper wallet, not connected to the network (offline), in which the private key of the virtual currency is stored. For both hardware and paper wallets, the issue is that the private key is not under the control of any specific entity other than the owner/holder of the wallet, and thus that entity can determine the virtual currency according to the public key of the blockchain, i.e. the accounting entry (amount) of that virtual currency. A cold wallet could be simplified to a form of storage where the storage of virtual currencies according to the public key takes place *without an external wallet service provider*.
6. In the draft bill, it is explicitly indicated that the system should be centralised and, on the one hand, the system should have an identifiable entity that acts as a representative of the virtual currency in a somewhat similar way to how a board of directors acts in an organisation (The Finnish Government, 2018).
7. Regarding the prevention of virtual currency money laundering and the financing of terrorism and the inadequacy of the means of AMLD5, e.g. by Schmidt and Hoube and Snyers (Houben and Snyers, 2018) (Schmidt, 2021). On the one hand, Turtiainen and Cox have written more generally about preventing money laundering and terrorist financing (Cox, 2014) (Turtiainen, 2018).
8. For example, the Supreme Administrative Court of Finland 1992 B 501, the Supreme Administrative Court of Finland 1984 II 506 and the Supreme Administrative Court of Finland 1973 T 425.
9. However, it should be noted that in all situations the virtual currency provider does not necessarily meet the business criteria, even if the obligation to know the customer is met in other respects.

References

Chainalysis (2022), "DeFi takes on bigger role in money laundering but small group of centralized services still dominate", [Online].

Chase, B. and MacBrough, E. (2018), "Analysis of the XRP ledger consensus protocol", arXiv:1802.07242, pp. 1-25.

Cox, D. (2014), *Handbook of Anti Money Laundering*, Wiley, Chichester.

FYFY (2021), "Fyfy: pre-ICO event., s.l", YouTube.

Houben, R. and Snyers, A. (2018), *Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*, European Union, Brussels.

Keskitalo, K. (2022a), "Legal history of regulation of money – the legal concept of money before and now", University of Helsinki Faculty of Law.

Keskitalo, K. (2022b), "Virtual currency mining: earnings or capital income?", Edilex, Issue 7.

Keskitalo, K. and Väyrynen, J. (2022), "The virtual currency provider's duty to customer due diligence: special issues concerning the issuer", *Liikejuridiikka*, No. 3, pp. 48-67.

Ministry of Finance (2018), "Memorandum: implementation of the 2018 amending directive to the EU's fourth money laundering directive (Fi2018/03025/B)", s.l.:s.n.

Schmidt, A. (2021), "Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model get access arrow", *International Journal of Law and Information Technology*, Vol. 29 No. 4, pp. 332-363.

The Finnish Government (2008), "The government's proposal to the parliament for a law on preventing and investigating money laundering and terrorist financing and for some related laws 25/2008", s.l.:s.n.

The Finnish Government (2018), "The government's proposal to the parliament for a law on the supervision system of bank and payment accounts and some related laws 167/2018", s.l.: s.n.

The Guardian (2022), "Crypto exchange FTX owes nearly $3.1bn to 50 biggest creditors", (accessed 28 11 2022).

The Swedish Financial Supervisory Authority (2018), "Referral response: implementation of the 2018 amending directive to the EU's fourth money laundering directive (Fi2018/03025/B)", s.l.:s.n.

Turtiainen, M. (2018), *Investment Services and the Customer*, Alma Talent, Helsinki.

United Nations Office on Drugs and Crime (2022), "Money laundering. [online]".

Corresponding author
Kristian Keskitalo can be contacted at: kristian.keskitalo@helsinki.fi