GLIMSTEDT

Law firm GLIMSTEDT
Kai 1, 10111 Tallinn, Estonia
Tel. +372 611 8050, fax +372 611 8051
tallinn@glimstedt.ee www.glimstedt.ee

European Commission
(Attn: Secretary-General)
B-1049 Brussels
BELGIUM

14 September 2016

Sent by fax: 3222964335

CONTACT DETAILS OF THE REPRESENTATIVE

First Name: **Priit**
Surname: **Lätt**

Law firm GLIMSTEDT (in Estonian *Advokaadibüroo GLIMSTEDT*)
Address: Kai 1, Tallinn, Estonia
Post code: 10111
Phone: +372 611 8050
Fax: +372 611 8051
Registry code: 11067332
E-mail: menetlus@glimstedt.ee

I am submitting this complaint on behalf of Otto Albert de Voogd (see below).

CONTACT DETAILS OF THE COMPLAINANT

First Name: **Otto Albert**
Surname: **de Voogd**

Address: Vihuri 1-37, 10311 Tallinn
Phone: + 372 538 36846
E-mail: otto@de-voogd.com

Please contact Law firm GLIMSTEDT in case any additional information is necessary.

COMPLAINT

FACTS AND BACKROUND

1. Otto Albert de Voogd (hereinafter the **complainant**) exchanged small amounts of bitcoins with friends and acquaintances in Estonia until 13.02.2014. Due to bitcoin's price volatility he wrote a Javascript program to calculate the current bitcoin price using market depth information gathered from the API offered by Mt. Gox and later Bitstamp. He registered the domain name btc.ee in Estonia and used it to host his price calculation script. The complainant operated for non-commercial purposes, and it was a hobby project to help friends and acquaintances to try bitcoin.

2. Before March 2014, there was no guidance on the legal and regulatory treatment of virtual currencies (hereinafter **VC**), incl. bitcoin, in Estonia[1] and even at the EU level. The Financial Intelligence Unit of the Police and Border Guard Board (hereinafter the **FIU**) also has admitted that they had not made their interpretation public: *We will public [sic] our opinion regarding the matter of bitcoins on our website soon. [...] and for your information we have not kept our opinion in [sic] secret – we just did not saw [sic] the need for composing something like that earlier*.[2]

3. On 13.02.2014, the complainant received an e-mail from the representative of FIU (Mr. Urmas Pai) according to which the FIU initiated national surveillance procedure under the Money Laundering and Terrorist Financing Prevention Act (hereinafter **RahaPTS**). Based on RahaPTS, FIU found that bitcoin is an alternative mean of payment and a person providing services related to bitcoin is to be deemed a financial institution. The complainant was threatened with a 3 year prison sentence and a 32,000 EUR fine for acting as a financial institution without activity licence. The complainant was subsequently asked by FIU to provide the evidence and information. The complainant immediately ceased all activities.

4. On 24.03.2014, FIU issued the complainant an injunction No 1-9/1011 (hereinafter the **injunction**) requiring the complainant in the framework of national surveillance to provide evidence and information about his activities regarding providing services related to bitcoin. FIU made an onerous decision against the complainant under national rules that are in violation of EU law. According to the injunction, state coercion shall be applied against the complainant and the complainant (a physical person) shall be treated more strictly than a financial institution (e.g. a bank), and therefore the complainant's activities would be subjected to a number of obligations arising from RahaPTS (incl. the requirement to meet customers face-to-face for small transactions). With the injunction, FIU required from the complainant information, the disclosure of which could lead to the attribution of his activity under the Penal Code § 372(2)3) ("Economic activities without activity license and prohibited economic activities"). A collection of data from a person, which may lead to his or her punishment, can be viewed as a breach of privilege against self-incrimination.

5. The complainant refused to provide any self-incriminating information, and challenged the injunction in all court levels of the Republic of Estonia. With its decision of 11.04.2016 in the administrative case No 3-3-1-75-15, the highest court of the Republic of Estonia - the Supreme Court - denied the complainant's action. The Supreme Court found that Directive 2005/60/EC (hereinafter **3AMLD**) does not regulate the status of the provider of services of alternative mean of payment, but Article 5 of 3AMLD allows the Member States to lay down stricter rules than provided in 3AMLD. However, the Supreme Court highlighted a number of issues in RahaPTS that need a clearer solution (please see paras 26-28 of the decision):

1) The applicable customer due diligence requirements should meet the principle of proportionality, taking into account the specifics of each activity and its risks in the particular field of area.
2) The Estonian legislator should consider amendment of the regulation in relation to the providers of alternative means of payment (e.g. bitcoin exchanges) in such a way that it responds to specific situations and ensures sufficient flexibility.

6. The complainant considers that RahaPTS § 6(2)4) and (4) are inconsistent with European Union law, specifically with Article 2(1), Article 4(1) and (2) of 3AMLD. 3AMLD does not deem a provider of services related to VCs as a financial institution or obliged entity, and the Member State is not permitted to arbitrarily extend the list of obliged entities provided in Article 2(2).

[1] As testified by this article where Kuno Rääk (member of board of Tavex Group, Estonia's biggest currency exchange operator and payment service provider) asks the Estonian state to provide clarity: http://majandus24.postimees.ee/2671592/tavid-kaalub-bitcoiniga-kauplemise-alustamist (only in Estonian).
[2] E-mail of Mr. Urmas Pai (dated 14.03.2014).

LEGAL CONTEXT

7. Article 2(1) of 3AMLD provides the list of entities whose activity is under the scope of 3AMLD. According to Article 4(1) of 3AMLD, "Member States shall ensure that the provisions of this Directive are extended in whole or in part to professions and to categories of undertakings, other than the institutions and persons referred to in Article 2(1), which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes". Article 4(2) of 3AMLD provides that "Where a Member State decides to extend the provisions of this Directive to professions and to categories of undertakings other than those referred to in Article 2(1), it shall inform the Commission thereof".

8. In order to transpose 3AMLD into Estonian national law, RahaPTS was passed on 19.12.2007 and it entered into force on 28.01.2008. RahaPTS § 3(1)2) provides that RahaPTS applies to the economic or professional activities of financial institutions. According to RahaPTS § 6(2)4), for the purposes of RahaPTS, the financial institution means, *inter alia*, "a provider of services of alternative means of payment". RahaPTS § 6(4) provides that "A provider of services of alternative means of payment is a person who in its economic or professional activities and through a communications, transfer or clearing system buys, sells or mediates funds of monetary value by which financial obligations can be performed or which can be exchanged for an official currency, but who is not a person specified in subsection (1) or a financial institution for the purposes of the Credit Institutions Act".

REASONS OF COMPLAINT

9. RahaPTS § 6(2)4) and (4) are in contradiction with 3AMLD:

1) Estonian legislation has introduced more stringent measures than the minimum requirements of 3AMLD, extending the circle of financial institutions that are obliged entities of the money laundering regulations in RahaPTS § 6(2)4) and § 6(4) to VC related service providers by the so-called "providers of the service of alternative means of payment" without any impact assessments and consultations with stakeholders. The Estonian relevant legal norms are not formulated in a clear and proportionate manner, leaving the VC market participants without the safeguards as set out in the Charter of Fundamental Rights.
2) The Republic of Estonia has failed to inform the Commission of the extension of the scope of 3AMLD to the providers of the services of alternative means of payment, being thus in violation of the notification obligation provided in Article 4(2) of 3AMLD.

10. One objective of 3AMLD and thus the objective of harmonization of the legislation of the Member States was to prevent the Member States from taking, for the protection of its financing systems, such action, which could be incompatible with the functioning of the internal market, and with the principle of the rule of law and the principle of Community public policy (reason 2 of 3AMLD). It is inconsistent to 3AMLD, if Member State extends the list of obliged entities and creates onerous provisions to professions and to categories of undertakings which are not active in the area, which is particularly likely to be used for money laundering or terrorist financing purposes. From the entry into force of 3AMLD, the Member States lacked the right on their own initiative to establish the limitations and requirements set out in 3AMLD (the due diligence measures applicable as regards to the customer, the record-keeping obligation, etc.) also for these professions and categories of undertakings that have not been expressly listed in Article 2 of 3AMLD. 3AMLD provides for the legislatures of the Member States both the lower and the upper limit of the regulation (maximum harmonization).

11. The only possibility for a Member State to expand the list of the entities covered with the requirements of 3AMLD is due to Article 4(1), according to which the provisions of 3AMLD can be extended to the professions and categories of undertakings, which are not the authorities and persons referred to in Article 2(1), but which are operating in the area, which is particularly likely to be used for money laundering and terrorist financing purposes. Buying, selling and brokering activities of VCs, incl. bitcoins, was not on 28.01.2008 (entry into force of RahaPTS), on 24.03.2014 (date of the injunction)

and is still not such an area, which might be "particularly likely to be used for money laundering or terrorist financing purposes." Subjecting such persons and activities to unusually strict anti-money laundering regulation does not comply with the clause provided in Article 4(1) for the following reasons:

1) The market volume of bitcoins is marginal – the total market volume of the VCs, of which bitcoins represent 90%, is around 4,3 billion EUR, which represents in total only 0,04% of the broad money supply of the whole eurozone (as of March 2014, a 9,893 trillion EUR).
2) The total value of all bitcoins varies between 3 and 8 billion EUR, of which only a fraction is ever used.
3) Even in 2016, VCs represent an innovative but rather small market. The European Central Bank in its last report on VCs (February 2015) concluded that VCs entail certain risks but do not at this point in time pose a threat to financial stability due to their still limited size – around 70,000 transactions (which represents a total of 0,03% of the retail payments of the whole Eurozone) are made daily on VC platforms, worth around 40 million EUR.
4) Even today there is no evidence to indicate that the use of bitcoins has been adopted by criminals involved in terrorism or the use of bitcoins has been incorporated into established money laundering techniques in Estonia.

12. According to reason 5 in 3AMLD, the recommendations of the Financial Action Task Force (hereinafter **FATF**) should be taken into account. In this context, it is important to note that at the time of adoption of RahaPTS (19.12.2007) and issue of the injunction (24.03.2014) FATF had not yet defined VCs nor made explicit recommendations in this area. On June 2015, the FATF issued a guidance for a risk-based approach to VCs calling for the regulation of VC exchanges and other network participants that operate as "gatekeepers" with the regulated fiat currency financial system.

13. Article 4(1) of 3AMLD must be interpreted as meaning that national legislation such as that at issue in these proceedings, adopted pursuant to the discretion which Article 4(1) of that directive grants the Member States, must be compatible with EU law, in particular the fundamental freedoms guaranteed by the Treaties. Whilst such national legislation designed to combat money laundering or terrorist financing pursues a legitimate aim capable of justifying a restriction on the fundamental freedoms and whilst to presume that exchange of VCs present a risk of money laundering or terrorist financing is appropriate for securing the attainment of that aim, that national legislation exceeds, however, what is necessary for the purpose of achieving the aim which it pursues, since these activities did not objectively present such a risk in 2008 or even in 2014.

14. On 20.05.2015, the European Parliament adopted a new, fourth directive on the risk of money laundering 2015/849 (hereinafter **4AMLD**). Since there was no EU-level common understanding of the nature and regulation of VCs, there are no provisions in 4AMLD for the regulation of VCs, and the list of the obliged entities has not been extended to the providers of services related to VC. If in 4AMLD it has not been necessary to include the providers of services related to VCs (incl. bitcoin) into the list of obligated persons, then, accordingly, in the opinion of the EU legislature, no such risks related to VC exist, at least at present, with the minimizing of which the directives relating to the risk of money laundering have been established. Insofar, the EU legislature has not considered the performance of transactions and provision of services related to VC to be an area of activity that might be particularly likely be used for money laundering or terrorist financing purposes.

15. Moreover, pursuant to Article 4(1) of 4AMLD, Member States shall take a risk-based approach to risk assessment. Thus, the EU legislature has also further stressed in the new regulation that Member States cannot extend the list of obligated persons arbitrarily or randomly, but only in the light of the conditions laid down in the Directive (cf. Article 4(1) of 3AMLD; Article 4(1) of 4AMLD). The Republic of Estonia has not, while including VCs and the related services into the list of obliged subjects, equalizing these persons with traditional financial institutions, performed any analysis or risk assessment. It cannot be considered credible, as if in the Republic of Estonia, the use of bitcoins would be at a greater risk of money laundering than in other EU Member States. For example, in accordance with the study "UK

national risk assessment of money laundering and terrorist financing" conducted in Great Britain in the second half of 2015, use of virtual money in money laundering and terrorist financing is a low-risk level: "The money laundering risk associated with digital currencies is **low**, though if the use of digital currencies was to become more prevalent in the UK this risk could rise. Digital currencies are currently **not a method by which terrorists raise or move money** out of the UK /.../." (Pg. 86, Section 9.29). If even in the world's financial centre, London, in 2015, the use of bitcoins is not considered a significant risk, even less was this risk likely in Estonia in 2014 or is likely today.

16. It was not until the beginning of 2016 when a discussion arose in the European Commission and the European Parliament regarding whether VCs should be regulated in any way in the EU law.

1) The European Parliament issued a press release on 26.04.2016, according to which the Economic and Monetary Affairs Committee of the parliament supported the creation of a relevant work group. The press release indicates that the task of the work group is still only the mapping of the situation and risk assessment, and on the basis of the information collected, making the decision on the need for regulation: "To avoid stifling innovation, we favor precautionary monitoring instead of pre-emptive regulation. But, IT innovations can spread very rapidly and become systemic. That's why we call on the Commission to establish a task force to monitor actively how the technology evolves and to make timely proposals for specific regulation if, and when, the need arises." The formation of a work group, and the ToRs given to it, indicate that VC is still not considered an area which is "particularly likely to be used for money laundering or terrorist financing purposes". Again, these developments confirm that the Republic of Estonia could not incorporate the providers of the services related to cryptocurrency into the list of obliged persons under 3AMLD, in so far as these individuals did not correspond then or do not correspond now to the conditions provided in the Article 4(1) of 3AMLD.
2) In its resolution of 26.05.2016 on virtual currencies (2016/2007(INI)), the European Parliament has, *inter alia*, called for a proportionate regulatory approach at EU level so as not to stifle innovation or add superfluous costs to it at this early stage, while taking seriously the regulatory challenges that the widespread use of VCs might pose (p 14); welcomed the Commission's suggestions for including VC exchange platforms in the 4AMLD in order to end the anonymity associated with such platforms (p 19); expected that any proposal in this regard will be targeted, justified by means of a full analysis of the risks associated with VCs, and based on a thorough impact assessment (p 19).
3) Finally, on 05.07.2016, the Commission made a proposal to amend Article 2 of 4AMLD in order to bring VC exchange platforms and custodian wallet providers under the scope of 4AMLD. For legal certainty reasons, the definition of VC was also proposed.

LEGAL ACTIONS IN MEMBER STATE

The complainant has taken action in Estonia to attempt to solve this problem. Namely, the complainant lodged an action to the administrative court, but judicial proceedings did not result in satisfactory solution. With its decision of 11.04.2016 in the administrative case No 3-3-1-75-15, the highest court of the Republic of Estonia dismissed the action. There are no cases pending before a court anymore regarding this issue.

REQUEST OF COMPLAINT

In accordance with the above mentioned, we hereby ask:

- **to accept the complaint for examination and open infringement proceedings against the Republic of Estonia.**

LIST OF DOCUMENTS

1. Injunction No 1-9/1011 of the Financial Intelligence Unit of the Police and Border Guard Board;
2. Ruling of 11 April 2015 of the Supreme Court in administrative case No 3-3-1-75-15.

TRANSFERRING COMPLAINT TO SOLVIT

No, the complainant does not agree to the Commission's transferring his complaint to SOLVIT.

CONFIDENTIALITY

The complainant authorises the Commission to disclose his identity in its contacts with the authorities of the Republic of Estonia.

Best regards,

Priit Lätt
Representative of the complainant
Attorney at Law / Partner
GLIMSTEDT