Regulatory alert for future Crypto-Assets Service Providers (CASPs):

EBA's consultation on the Revised Guidelines on money laundering and terrorist financing (ML/TF) risk factors

Timothy M. Bissessar
HVG Law – Regulatory & Blockchain Expert

HVG LAW

Introduction[1]

Most casual observers would of noticed that the Markets in Crypto Regulation (MiCA) was finalized and published in the EU Official Journal on 9 June 2023. As a result, the EU as a bloc, became the first place in the world to establish a comprehensive regulatory framework for crypto-assets. Also on 9 June and with far less fanfare, the recast of Regulation (EU) 2015/847 (Transfers of Funds Regulation, "TFR") was published in the EU Official Journal. The TFR recast extends the scope of the current TFR to the transfer of crypto-assets, which is in line with the Financial Action Task Force's (FATF) standards. The co-legislators reached a provisional agreement on the FTR recast on 29th June 2022. In this TFR recast ("Provisional Agreement") the European Banking Authority (EBA) was given ten legislative mandates, of which, four of them were related to topics that are to be addressed in the revised ML/TF Risk Factors Guidelines.

The four mandates tasked to EBA are:

a) determine the application of general enhance due diligence (EDD) to transfers of crypto-assets;
b) define possible EDD measures regarding transfers of crypto-assets involving self-hosted wallets;
c) define the criteria and elements to take into account for deciding EDD measures for correspondent banking relationships with non-EU CASPs; and
d) identify the risk variables and risk factors to be taken into account by CASPs when entering into business relationships or carrying out transactions in crypto- assets. Furthermore, Article 30(b) of the recast TFR amends article 3 of Directive (EU) 2015/849 (AML Directive or AMLD) to subject crypto-asset service providers (CASPs) to the same ML/TF requirements and ML/TF supervision as credit and financial institutions.

To meet these four mandates, EBA published on 31 May 2023 a public consultation on amendments to its Guidelines on money laundering and terrorist financing (ML/TF) risk factors ("ML/TF Risk Factors Guidelines", or "Guidelines")[2]. The proposed changes extend the scope of ML/TF Risk Factors Guidelines to crypto-asset service providers (CASPs). The consultation runs until 31 August 2023.

For the sake of completeness, note that in addition to the four EBA mandates above, the Provisional Agreement also mandated EBA through article 30[3] to issue guidelines, addressed to competent authorities, on the characteristics of a risk-based approach to supervision of crypto-asset service providers and the steps to be taken when conducting supervision on a risk-based basis. To meet this mandate, the EBA launched on 29 March 2023 a public consultation of its draft Guidelines amending the existing Risk-Based Supervision Guidelines[4]. The proposed changes extend the scope of these Guidelines to AML/CFT supervisors of CASPs. The consultation will run until 29 June 2023.

Furthermore, note that these (amended) Guidelines will be complemented with amendments to the Guidelines to prevent the abuse of fund transfers for ML/TF purposes[5], and new Guidelines on policies and procedures for compliance with restrictive measures.

In this article we outline the Guidelines and highlight the most relevant changes from a CASP perspective. Where possible at this early stage, we will also share our expectations regarding the potential impact of the revised Guidelines. Finally, note that the EBA will finalize these Guidelines once the consultation responses have been assessed. The publication of the final amending Guidelines is foreseen for Q4 2023/Q1 2024[6]. The EBA will consider whether changes to the content and scope of these amending Guidelines are needed.

[1] Note that the opinions expressed in this blogpost are solely that of the expert and may not be construed as legal advice.

[2] See link for consultation paper: https://www.eba.europa.eu/calendar/consultation-revised-guidelines-money-laundering-and-terrorist-financing-mltf-risk-factors.

[3] This is now article 36 under the TFR recast.

[4] See link for consultation paper: https://www.eba.europa.eu/calendar/consultation-draft-guidelines-amending-risk-based-supervision-guidelines.

[5] JC/GL/2017/16.

[6] Final date is subject to EBA's discretion.

Outline of the amended Guidelines & specific key considerations

The EBA is proposing to amend its ML/TF risk factors Guidelines to set common, regulatory expectations of the steps CASPs should take to identify and mitigate these risks effectively. The amendments introduce new sector-specific guidance for CASPs, which highlights factors that may indicate the CASP's exposure to the higher or lower ML/TF risk. Further to the consultation paper CASPs should consider these factors when carrying out the ML/TF risk assessments of their business and customers at the outset and during the business relationship. The Guidelines also explain how they should adjust their customer due diligence (CDD) in line with those risks. Furthermore, the amendments include guidance to other credit and financial institutions on risks to consider when engaging in a business relationship with a CASP or when they are otherwise exposed to crypto assets. See below a general outline of the amendments relevant for firms, in particular for CASPs:

General amendments (Guidelines 1 – 6):

- **Guideline 1.7** - the scope of the revised ML/TF Risk Factors Guidelines is currently related to credit and financial institutions (altogether "the firms"), with article 38 TFR recast and the amendment of article 3 of AMLD, CASPs are included in the 'financial institutions' definition and, de facto, included in the Guidelines. Guideline 1.7 clarifies that CASPs are in scope for the application of the Guidelines, as do other institutions.
  As such, CASPs are to carry out ML/TF risk assessments before launching new products or services, as well as change their practices.
- **Guideline 2.4** - on the identification of ML/TF risk factors specifies what obliged entities must consider when carrying out their risk assessments. Exposure to certain crypto-asset activities, especially unregulated ones, is added as a risk-increase factor.
- **Guideline 4.29** - on customer due diligence (CDD) the Guideline recognizes that CASPs onboard their customers through remote solutions and therefore must ensure compliance with the EBA Guidelines on Remote Customer Onboarding[7]. These Guidelines apply to all obliged entities using remote innovative solutions for customer onboarding.
- **Guideline 4.60** – this Guideline was amended to reflect the "red flag" indicators to be considered by CASPs. The amended Guideline follows the 2020 recommendations from the Financial Action Task Force (FATF) and proposes the following indicators: (i) the frequency of small amount transactions; and (ii) successive transactions without obvious economic rationale.
- **Guideline 4.74** – This Guideline emphasizes the need for adequate transaction monitoring systems, with advanced analytical tools, should also be put in place and specify that, in some circumstances, advanced analytics tools might be warranted due to the level of ML/TF risks.
- **Guideline 6.2** - This Guideline highlights the need for some staff to undergo training of a more technical nature to ensure that they are able to interpret the outcomes of the monitoring systems used by the firm, in particular where advanced analytics tools are used.

[7] EBA/GL/2022/15; see link https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-15%20GL%20on%20remote%20customer%20onboarding/1043884/Guidelines%20on%20the%20use%20of%20Remote%20Customer%20Onboarding%20Solutions.pdf

Sectoral guidance: correspondent relationships, retail banks, e-money and investment firms and crowdfunding (Guidelines 8, 9, 10, 15 and 17):

Guideline 8 - Following article 38(2) of the Provisional Agreement, guideline 8 stresses that the Guidelines for firms offering correspondent relationship services also apply to CASPs, including the CDD measures that should be applied to mitigate the risks.

Guidelines 8.6 & 8.8 – These Guidelines identify what is to be considered a higher risk activity for respondent conducts. Business on behalf of third-country CASPs not regulated under MiCA and business on behalf of CASPs which allow transfers to and from self-hosted addresses are included on the list. For factors that can contribute to increase risk, the following are added under Guideline 8.6:
i) the IBAN provided by a respondent CASP to receive fiat funds from customers is in the name of a company other than the CASP[8]; and ii) the respondent is unable to verify with sufficient certainty that customers are not based in high-risk jurisdictions, including when the IP address of the customer is unverifiable, in circumstances where it is required by the respondent's policies and procedures[9].

Guideline 9 – Regarding sectorial guidance for retail banks, Guideline 9 highlights that some providers of crypto-asset services still remain outside the regulatory scope – in the EU and abroad – and thus can present additional ML/TF risks.

Guideline 9.16 is e.g. amended as follows: for bank customers opening pooled/omnibus accounts for funds or crypto-assets that belong to the customer's own clients, banks are to apply full CDD measures. Simplified DD can be applied, in certain situations and if allowed by national law, as applicable to other firms as well.

Guidelines 9.20 to 9.23, "Customers that offer services related to virtual currencies" – These amendments ensure that the Guidelines are aligned with MiCA/TFR recast on their concepts. Moreover, banks are to apply, amongst others, the following mitigating CDD measures: i) enter into dialogue with the customer to understand the nature of the business and the ML/TF risks to which it is exposed; ii) carry out due diligence on senior management, including consideration of any adverse information; iii) understand the extent to which these customers apply their own CDD measures; and iv) assess whether the businesses issuing crypto-assets to raise funds are legitimate and regulated.

The amended Guidelines 10 and 15 – These Guidelines clarify that CASPs should also consider Guideline 21 on specific guidance for CASPs.

Guideline 17 - proposed amendments replace references to "virtual currencies" with references to "crypto assets".

[8] See newly added Guideline 8.6 (h).

9 See newly added Guideline 8.8(d).

Sectoral Guidance for CASPs (Guideline 21) NEW

General regulatory expectations - This new Guideline provides the regulatory expectations for CASPs when they identify and assess ML/TF risks associated with their overall business and with individual business relationships. In particular, Guideline 21 determined that transactions with self-hosted addresses or other services/products offered by CASPs that entail privacy-enhancing features or offer a higher degree of anonymity may expose them to increased higher ML/TF risks. The EBA also stresses that the global nature of CASPs' business models may present heightened ML/TF risks, particularly where CASPs' customers are transacting with jurisdictions associated with a high risk of ML/TF.

Guideline 21.3 - Products, services and transactions risk factors: According to this Guideline the following factors may contribute to risk-increasing:

a) privacy-enhancing features;
b) payment transactions with no apparent economic rationale;
c) products with no limit on overall volume/value of transactions;
d) products that allow transactions between the customer's account and:
   (i) self-hosted wallets;
   (ii) unregulated and/or third-country unregulated providers;
   (iii) peer-to-peer crypto exchanges and tumbler platforms;
   (iv) defi structures; and
   (v) crypto-ATMs and other hardware outside the regulatory and supervisory EU regime.
e) products involving new business practices and the use of technologies where the level of the ML/TF risk is not fully understood by the CASP; and
f) where the CASP is offering nested services[10] of a wholesale CASP where the wholesale CASP exercises only weak control over the nested service.

Guideline 21.4 - Products, services and transactions risk factors: According to this Guideline the following factors may contribute to risk-increasing:

a) products with reduced functionality, such as low transaction volumes or values;
b) the product permits transactions between the customer's account and:
   i) crypto-asset accounts in the customer's name held by a CASP;
   ii) crypto-asset accounts in the customer's name held by regulated third-country providers[11]; and
   iii) a bank account in the customer's name at a credit institution that is subject to either the AMLD framework or another framework outside the EU that is as robust as the AMLD framework.
c) nature and scope of the payment channels used by the CASP is limited to closed loop systems or systems intended for micro-payments or government-to-person or person-to-government payment; and
d) the product is available only to certain categories of customers, like employees of a company.

[10] I.e. a service within a service.
[11] Provided said third-country regulatory framework is as robust as that of MiCA and which is subject to a AML/CFT framework which is equally robust as the one provided for in AMLD.

Guideline 21.5 - Customer risk factors: the Guideline also looks to the nature of the customer, noting as high risk amongst others, undertakings which are in intra-group relationships with other crypto-asset business;
IP addresses associated with a darknet or other encryption methods including VPNs; and vulnerable people who display little knowledge of crypto-assets and associated technology. The Guideline also looks at factors regarding the customer's behavior, e.g. situations where the customer tries to open multiple crypto-asset accounts with the CASP; customer's UBO[12] is unwilling or unable to provide the necessary CDD information, without any legitimate reason; a customer which uses an IP address or mobile device linked to multiple customers without any apparent economic reason and frequently changes its personal information.

Guideline 21.6 - Customer risk reduction factors: Where the customer has e.g. complied with the TFR recast, travel rule requirements during previous transactions in crypto-assets and is well known to the CASP through previous business relationships.

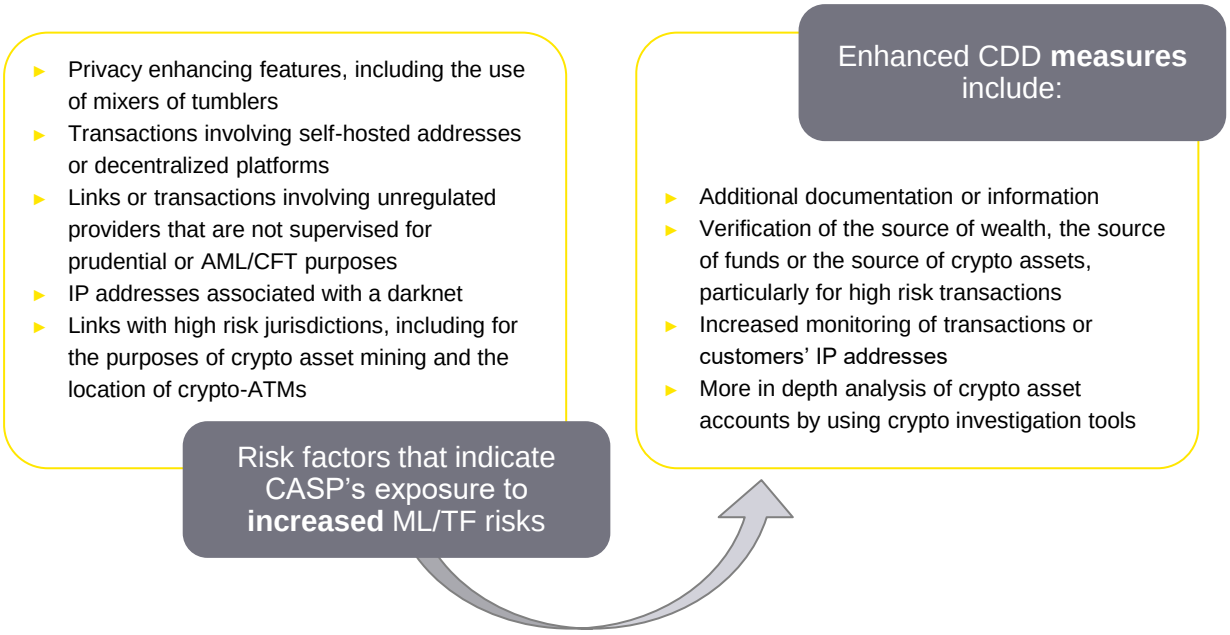
Guideline 21.7 - Country/geographical risk factors: Some of these factors are, the customer's funds that are exchanged to crypto-assets are derived from links to jurisdictions associated with higher ML/TF risk and the customer is involved in crypto-asset mining operations that take place in a high-risk jurisdiction[13]. Guideline 21.8 contains the single geographical risk reduction factor.

Guideline 21.9 – Distribution channel risk factors: Some of these factors are where the business relationship is established by using remote customer onboarding solutions that are not compliant with EBA's guidelines on remote customer onboarding and where the new distribution channels have not been fully tested yet or used before. Guideline 21.10 contains the single distribution channel risk reduction factor.

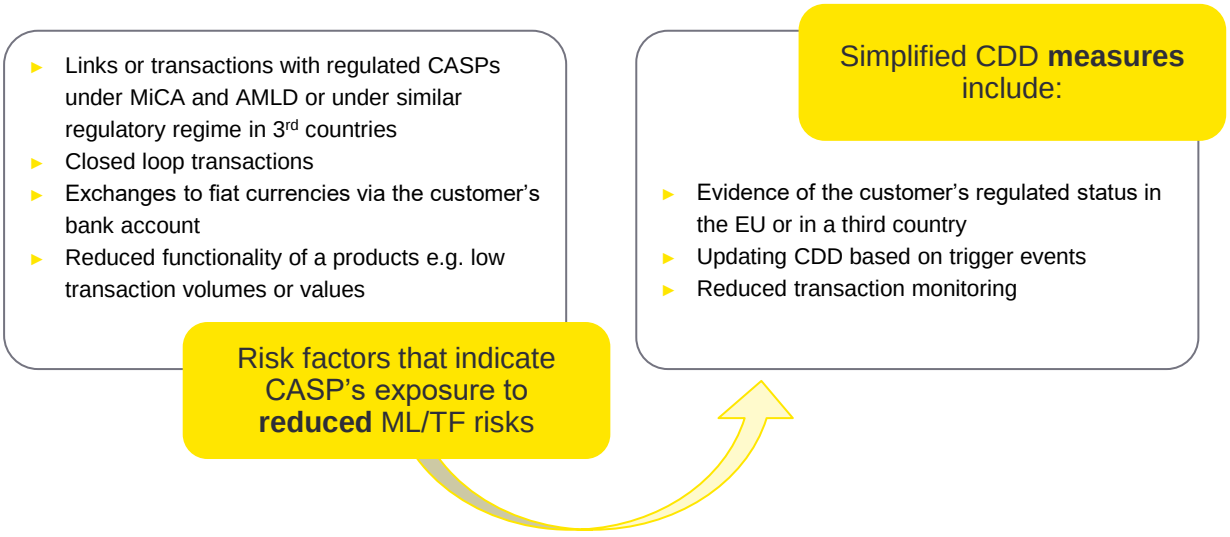
Guidelines 21.12-21.14 for enhanced CDD measures and Guideline 21.15 for simplified CDD measures - The new Guideline also sets out the enhanced and simplified CDD measures to be applied by CASPs to business relationships, which are exposed to increased or low risk of ML/TF. These fall fairly close to the measures to be applied by other firms with two notable differences: i) CASPs are required to have adequate systems to monitor all types of crypto-assets; and ii) CASPs should determine the circumstances where the use of advanced analytics tools is warranted for their business.

[12] Ultimate beneficial owner
[13] As identified by the European Commission further to article 9 AMLD.

High risk factors resulting Enhanced CDD measures



Reduced risk factors resulting Simplified CDD measures



Guidelines 21.16 – Record Keeping: This Guideline stipulates where the information on customers and transaction is available on the distributed ledger, firms should not place reliance on the distributed ledger for recordkeeping but should take steps to fulfil their recordkeeping responsibilities in accordance with AMLD and Guidelines 5.1 and 5.2.

In conclusion

The proposed changes extend the scope of the Guidelines to CASPs. The EBA proposes to amend the guidelines to set common regulatory expectations of the steps CASPs should take to identify and mitigate risks effectively. The amendments, inter alia, introduce new sector-specific guidance for CASPs and highlight factors that may indicate a CASP's exposure to increased or lower ML/TF risk.

We recommend future CASPs (i.e. either current VASPs converting into CASPs or new aspirant CASPs) to take the following into account when determining how to comply with the Guidelines:

- CASPs should consider the different risk factors when carrying out the ML/TF risk assessments of their business and customers at the outset and during the business relationship. Compliance by design is therefore key here.
- CASPs should also ensure that their systems, policies and procedures at the outset are capable to adjust their CDD levels further to the different risks factors; and
- Other firms than CASPs subject to the Guidelines should start considering these CASP-specific risk factors when engaging in a business relationship with a CASP or when they are exposed to crypto- assets.

What HVG Law can do for you

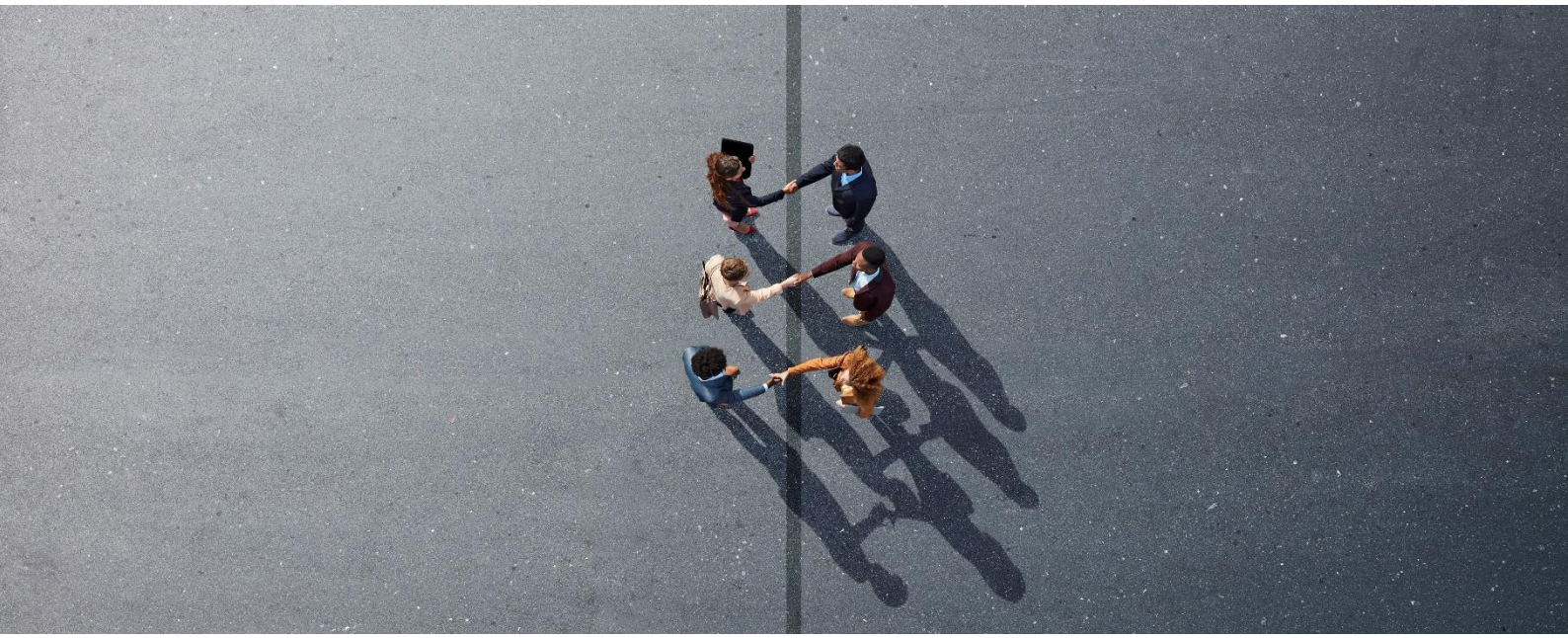
HVG Law has provided legal advice within this landscape since 2015, and HVG Law together with EY are happy to assist you with legal, strategic, business, legal, regulatory, compliance and tax challenges as well as opportunities that may arise from the world of cryptocurrencies. See below an overview of some of the topics on how HVG Law and EY can help your firm with respect to TFR and MiCA compliance.

Tax/Legal

- Tax reporting including CARF gap analysis and implementation
- VAT support
- Support in the corporate setup of Dutch VASPs/CASPs
- Transfer pricing support and documentation
- CASP licensing and MiCA/TFR regulatory compliance
- Assistance with complying with the amended AML/CFT rules for CASPs further to the Guidelines
- Full regulatory and legal support, including analysis of business plans, intended activities and/or products, filings at financial regulatory authorities and implementation of business strategy

Consulting

- Strategy definition and product development (e.g., tokenisation, development of ARTs)
- Preparation and/or review of white papers
- MiCA/TFR gap analysis
- Cybersecurity, DORA and outsourcing assessments
- Compliance/Crypto-related training to staff members



Our Dutch Blockchain team

HVG Law

Timothy Bissessar

Financial & Blockchain Regulatory Expert | Financial Services Regulation

Mobile: +316 21 25 23 20
timothy.bissessar@hvglaw.nl

Gijs van de Wouw

Partner | Finance Law & HVG Law Blockchain Leader

Mobile: +316 29 08 39 68
gijs.van.de.wouw@hvglaw.nl

EY Tax

Dennis Post

Partner | Advanced Technology Tax Lab

Mobile: +316 29 08 33 27
dennis.post@nl.ey.com

EY-Parthenon

Igor Mikhalev

Partner | Emerging Technologies

Mobile: +316 83 59 08 19
Igor.Mikhalev@parthenon.ey.com

About HVG Law
HVG Law LLP (HVG Law) ranks amongst the top Dutch law firms and is characterized by an entrepreneurial, innovative and solution-driven approach. With more than 150 dedicated and pragmatic lawyers, including (candidate) Civil Law Notaries, HVG Law offers high-quality, legal services in a broad and multidisciplinary context. Our lawyers are active in all legal areas and sectors relevant to business, directors, shareholders and government authorities and have knowledge of your business and your market. At our offices in Amsterdam, Rotterdam, Utrecht, Eindhoven, New York, Chicago and San Jose (i.e., Donahue & Partners LLP in the USA), we are able to offer our legal services to national and international clients.