NETHERLANDS

Jeroen Bos, Koen van Leeuwen, Marise Kok

(Simmons & Simmons)

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1. What is the general state of fintech innovation in your jurisdiction?

Fintech innovation in the Netherlands continues to develop. There has been a high level of activity in the fields of artificial intelligence, machine learning, blockchain, mobile and advanced analytics. The Dutch market is also adopting other innovations such as open banking (as a result of Directive (EU) 2015/2366 (second Payment Services Directive)).

Generally, diversification in the Dutch financial services sector has increased due to new entrants entering the market and incumbents (such as large Dutch banks) progressing their own fintech initiatives. However, increasing regulatory scrutiny and supervisory costs seems to deter new entrants into the market. Nevertheless, despite the additional administrative and compliance costs of the Dutch registration regime for certain crypto service providers that applies since May 2020, nearly 40 crypto service providers are registered to date.

Government and regulatory support

2. Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

In June 2016, the Dutch Authority for the Financial Markets (AFM) and the Dutch Central Bank (DNB) set up the InnovationHub to provide new and existing firms with support in answering queries related to the regulation of innovative financial products and services. The Innovation Hub is a joint information desk of the AFM, DNB and the Dutch Authority for Consumers

and Markets (ACM). It aims to offer easy access to supervisors and regulators for companies that provide innovative services or products, gain more insight into the rapidly developing technological innovation within the financial sector, and improve knowledge, sharing and dialogue with all relevant stakeholders. Firms can submit specific questions through the Innovation Hub, to which DNB, the AFM and the ACM provide informal answers.

In 2016, the AFM and DNB set up the Regulatory Sandbox for fintech companies to test and develop new products. If certain criteria are met, the Regulatory Sandbox can provide bespoke solutions for financial services companies that cannot reasonably meet specific policies, rules or regulations when marketing an innovative product, service or business model, but that do meet the underlying rationale of these policies, rules or regulations. The Regulatory Sandbox was evaluated as part of the discussions taking place in the iForum.

The DNB also periodically organizes the Fintech meets the Regulator seminar, during which relevant market participants and the DNB share thoughts on current developments.

Additionally, in November 2019, the DNB launched the iForum, a platform for joint initiatives intending to create value for the Dutch sector and the DNB. Through the iForum, the Dutch sector and the DNB can have a dialogue on the impact of technological innovations on the sector and develop joint pilots and experiments.

In October 2021, the ACM, the AFM, the Dutch Data Protection Authority (AP) and the Dutch Media Authority (CvdM) established the Digital Regulation Cooperation Platform (SDT). The SDT wishes to gain more insight into the online use of personal data by algorithms, among other things, and will coordinate how to enforce (new) EU rules and regulations on digitalization. For example, this includes new rules and regulations on dealing with large technology companies, the data economy and the platform economy (such as

the Digital Services Act, the Digital Markets Act, the Data Governance Act and the Artificial Intelligence Act).

There are no formal arrangements with foreign regulators that relate specifically to fintech companies. However, both the AFM and the DNB maintain contact with other regulators in the Netherlands (such as the ACM, the AP and the CvdM), the European Union and globally (such as the International Organization of Securities Commissions).

FINANCIAL REGULATION

Regulatory bodies

3. Which bodies regulate the provision of fintech products and services?

There is no specific regulatory framework applicable to the provision of fintech products and services, besides the registration regime for certain crypto service providers. Such crypto-service providers are supervised by the Dutch Central Bank (DNB).

As such, depending on the nature and scope of products and services offered, the Dutch Authority for the Financial Markets (AFM) and the DNB supervise compliance with the conduct of business rules and prudential requirements respectively.

Regulated activities

4. Which activities trigger a licensing requirement in your jurisdiction?

Depending on the nature and scope of services offered, licensing requirements under the Dutch Financial Supervision Act (FSA) and secondary legislation may apply.

The following activities are regulated under the FSA:

- deposit-taking and extension of credit for one's own account: credit institutions (ie, institutions that attract repayable funds from the public in the Netherlands and that extend credit for own account) require a banking licence.
- consumer lending: the extension of credit to consumers (natural persons acting outside their business or profession) requires a licence.
- factoring, to the extent this would constitute consumer lending.
- invoice discounting, to the extent this would constitute consumer lending.
- payment services: all institutions carrying out payment services as described in the Annex to Directive (EU) 2015/2366 (second Payment Services Directive) (PSD2), require a licence. A licence to act as a credit institution may also cover carrying out payment services.
- investment services: a financial institution is required to have a licence if it intends to provide investment services. These can be split into the following services, carried out in pursuit of a business or profession:
    - receiving and transmitting client orders relating to financial instruments (which includes bringing about deals in financial instruments);
    - executing client orders relating to financial instruments;
    - managing an individual's assets;
    - providing advice regarding financial instruments;
    - underwriting or placement with a firm commitment basis of financial instruments; and
    - placement without a firm commitment basis of financial

instruments; and

- investment activities: a financial institution is required to have a licence if it intends to perform an investment activity. Investment activities can be split into three activities:
    - dealing on one's own account (including foreign exchange trading);
    - operating an organized trading facility; and
    - operating a multilateral trading facility; and
- clearing and settlement: acting as a clearing and settlement institution requires a licence; and
- secondary market loan trading.

The registration regime for certain crypto service providers follows from the Dutch Money Laundering and Terrorist Financing (Prevention) Act. This regime only applies to crypto service providers that provide exchange services between fiat currencies and virtual currencies and (or) provide custodian wallet services for virtual currencies.

Consumer lending

5. Is consumer lending regulated in your jurisdiction?

Under the FSA, consumer lending requires a licence. Consumer credit is considered a financial product. Advising a consumer on a financial product or providing intermediary services in relation to such a financial product is only permitted if the institution has obtained a licence from the AFM. Financial institutions may be exempted if they have another licence that permits consumer lending or advising consumers on financial products.

Before entering a loan agreement with a consumer, the financial institution must provide the consumer with relevant information relating to the financial

product, so that the consumer is able to properly assess the product. In addition, credit assessment rules exist to prevent consumer over-indebtedness. These rules are part of the overarching requirement that lenders exercise due care when providing these services.

Secondary market loan trading

6. Are there restrictions on trading loans in the secondary market in your jurisdiction?

Secondary market loan trading is only a regulated activity where it constitutes consumer lending.

Collective investment schemes

7. Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

In the FSA, collective investment schemes can be an alternative investment fund, as defined in Directive 2011/61/EU (Alternative Investment Fund Managers Directive) (AIFMD), or an undertaking for collective investment in transferable securities, as defined in Directive 2009/65/EC Undertakings for Collective Investment in Transferable Securities Directive (UCITSD).

Under the AIFMD, an alternative investment fund is a vehicle with or without legal personality, which raises capital from investors with a view to investing it in accordance with a defined investment policy for the benefit of those investors. The AFM has confirmed that firms offering units in funds that invest in cryptocurrencies require a licence as an AIFM.

Whether a fintech company qualifies as a collective investment scheme depends on the exact nature of its business. For example, fintech companies that manage assets on a pooled basis on behalf of investors should give particular consideration as to whether they qualify as a collective investment

scheme. On the other hand, fintech companies that provide advice or payment services may be less likely to constitute a collective investment scheme. Peer-to-peer lenders, marketplace lenders or crowdfunding platforms could potentially fall within the scope of the AIFMD, to the extent they would qualify as (managers of) collective investment schemes.

Alternative investment funds

8. Are managers of alternative investment funds regulated?

Yes. Managers of alternative investment funds are regulated under the AIFMD, which has been implemented in the FSA.

Peer-to-peer and marketplace lending

9. Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

There is no specific regulation of peer-to-peer (P2P) or marketplace lending in the Netherlands. However, this activity might constitute a regulated activity under the FSA. For instance, if a platform facilitating P2P lending receives and transmits orders in financial instruments, it may be subject to a licensing obligation as an investment firm.

Crowdfunding

10. Describe any specific regulation of crowdfunding in your jurisdiction.

As of 10 November 2021, the EU Crowdfunding Regulation applies. Among other things, this Regulation introduced a licensing regime for crowdfunding service providers (CSPs) that:

- facilitate granting of loans excluding consumer credit (loan-based crowdfunding); or

- place without a firm commitment basis transferable securities and instruments issued by project owners or SPVs, and receive and transmit orders for crowdfunding purposes (equity-based crowdfunding).

However, if crowdfunding offers made by a particular project owner exceed €5 million over a period of 12 months, then the licensing regime for investment firms under Directive 2014/65/EU (Markets in Financial Instruments Directive II) (MiFID 2) applies instead.

CSPs that were permitted to provide crowdfunding services in the Netherlands before 10 November 2021 can avail themselves of a transitional regime under which they are permitted to continue doing so until 10 November 2022. This transitional period has been extended by one year until 10 November 2023.

After this date, CSPs require a licence from the AFM under the EU Crowdfunding Regulation. The AFM encourages CSPs to already apply for such licence, regardless of the above-mentioned extension of the transitional period.

Invoice trading

11. Describe any specific regulation of invoice trading in your jurisdiction.

There is no specific regulation of invoice trading in the Netherlands. However, depending on the exact services provided and the status of the parties involved, invoice trading may lead to either party qualifying as an intermediary of consumer credit or may amount to the extension of consumer credit.

Payment services

12. Are payment services regulated in your jurisdiction?

Yes. In the Netherlands, payment services are regulated based on PSD2, which has been implemented in the FSA. A licence is required to carry out all

payment services listed in the Annex to PSD2.

Payment services include:

- services enabling cash to be placed on a payment account or cash withdrawals from a payment account and all the operations required for operating a payment account;
- the execution of the following types of payment transactions:
    - direct debits, including one-off direct debits;
    - payment transactions executed through a payment card or a similar device; and
    - credit transfers, including standing orders; and
- the execution of the following types of payment transactions where the funds are covered by a credit line for the payment service user:
    - direct debits, including one-off direct debits;
    - payment transactions executed through a payment card or a similar device; and
    - credit transfers, including standing orders; and
- issuing payment instruments or acquiring payment transactions;
- money remittance;
- payment initiation services (initiating a payment order at the request of a payment service user with respect to an account held with another payment service provider); and
- account information services (online services to provide consolidated information on one or more payment accounts held by the payment

service user with another one (or more) payment service provider).

Open banking

13. Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

The implementation in the FSA of the access-to-account rules, as included in the PSD2, requires financial institutions to provide access to the payment accounts of clients to payment initiation service providers and account information service providers. In general, data protection and privacy regulations should be considered prior to making client data available to third parties.

Robo-advice

14. Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Currently, there is no specific regulatory framework for robo-advisers in the Netherlands.

As such, there is no legal distinction between robo-advice and traditional investment advice in the Netherlands. Therefore, companies providing robo-advice must – in principle – fulfil the same legal requirements as companies providing traditional investment advice.

However, the AFM has issued two documents relating to robo-advice:

- the AFM's view on robo-advice, in which the AFM discusses the duty of care and points of attention specifically in relation to robo-advice on mortgage loans and occupational disability insurance (but also in relation to other high-impact financial products). In general, the AFM

states that while robo-advice could be an opportunity to improve both access and the quality of investment advice, there are also specific points of attention to consider, including:

    - determining for which target group robo-advice is suitable;
    - determining which financial products are included in the robo-advice;
    - the algorithm’s ability to identify when clients have doubts;
    - detection of contradictory client answers; and
    - explanations on the product features and advice; and

- guidelines for (semi)-automated portfolio management, in which the AFM provides guidance regarding the (technique-neutral) duty of care of asset managers who offer semi-automatic investment advice and portfolio management. These guidelines are not legally binding but they do bring clarity for asset managers. The guidelines are aligned with Dutch law, MiFID 2 and suitability guidelines published by the European Securities and Markets Authority and set out, among other things, guidance on safety and the provision of information.

Additionally, on 1 July 2020, Dutch draft legislation on automated advice was published as part of a publication consultation. This legislation aims to introduce safeguards to ensure adequate provision of automated advice. In this context, the legislation:

- applies competence requirements to automated advice;
- requires that two individuals are responsible for the automated system and advice; and
- imposes rules on controls and systems.

This legislation targets automated advice on financial products in general. On 3 May 2023, the Dutch Council of State issued its advice on this draft legislation.

At this moment, there is no specific regulation of other companies that provides retail customers with automated access to investment products in the Netherlands. There is no legal distinction between companies providing automated access to investment products and companies that offer investment products in a traditional way.

Insurance products

15. Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes. The sale of insurance products is regulated under the FSA and requires a licence.

Credit references

16. Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The rules on credit rating agencies laid down in Regulation (EC) No. 1060/2009 on credit rating agencies (as amended) apply in the Netherlands. A credit rating agency is required to adopt, implement and enforce adequate measures to ensure that the credit ratings it issues are based on a thorough analysis of all the information that is available to it and is relevant to its analysis according to its rating methodologies.

CROSS-BORDER REGULATION

Passporting

17. Can regulated activities be passported into your jurisdiction?

An EEA firm that has been authorized under one of the EU single market

directives (Directive 2013/36/EU (Capital Requirements Directive), Directive 138/2009/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (Recast), Directive 2014/65/EU (Markets in Financial Instruments Directive II), Directive (EU) 2016/97 (Insurance Distribution Directive) (Recast), Directive 2014/17/EU (Mortgage Credit Directive), Directive 2009/65/EC Undertakings for Collective Investment in Transferable Securities Directive, Directive 2011/61/EU (Alternative Investment Fund Managers Directive) and Directive (EU) 2015/2366 (second Payment Services Directive) may, in principle, provide cross-border services into or establish a branch in the Netherlands. This also applies to an EEA firm authorized as a crowdfunding service provider under Regulation (EU) 2020/1503 on European Crowdfunding Service Providers.

To exercise this right, in general, the firm must first provide notice to its home state regulator. The relevant directive under which the EEA firm is seeking to exercise its passporting rights as implemented in the Dutch Financial Supervision Act (FSA) will determine the conditions and processes that the EEA firm must follow.

Crypto service providers registered elsewhere in the EEA for the provision of exchange services between virtual and fiat currencies, and custodian wallet services currently cannot passport their services into the Netherlands.

Requirement for a local presence

18. Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

To obtain a licence for any of the activities regulated pursuant to the FSA; in general, a local presence must be established, unless a firm can benefit from a European passport or a specific cross-border licensing regime is available.

SALES AND MARKETING

Restrictions

19. What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Depending on the regulatory status of the financial institution, different marketing rules may apply, including clientele restrictions. Advice should be sought on the specific circumstances of any particular case.

The Dutch Financial Supervision Act (FSA) states that, in general, relevant marketing activities:

- must be correct, clear and not misleading;
- must be recognizable as being of a commercial nature (where applicable); and
- may not contradict the information that is required to be made available pursuant to the FSA.

In addition, specific rules apply depending on the type of product offered or service provided and, in some cases, also on the type of client targeted. Some of these are summarized below.

Marketing materials for complex products (eg, participation rights in an open-ended collective investment scheme and investment objects) should include a risk indicator as prescribed by the Dutch Further Regulation on Conduct of Business Supervision of Financial Undertakings (the Further Regulation).

Marketing materials for credit offerings to consumers that refer to debit interest rates or other information regarding costs should include (at a minimum) information regarding floating or fixed interest rates and other costs that form part of the total costs of the credit for the consumer, the total credit amount, the yearly cost percentage, identity and address of the provider or intermediary, and

certain other information depending on the type of credit, all as prescribed in the Decree on Conduct of Business Supervision of Financial Undertakings.

In addition, certain risk warnings are prescribed and certain prohibitions apply, such as the prohibition on including any references to the speed or ease with which the credit may be obtained.

For products other than complex products, general marketing rules included in the Further Regulation apply, including the obligation to include a warning that the value of an investment may fluctuate and that historical returns offer no guarantee for the future.

Depending on the medium used for marketing (print, TV, radio or internet) further rules apply, such as the relevant information to be included at a minimum (namely, the name of the provider, the regulatory status of the provider, and where and how further information relating to the product or service can be obtained). Specific marketing rules have been introduced to facilitate marketing on social media.

Further, the Dutch Authority for the Financial Markets (AFM) has imposed a ban on the selling, marketing or distribution of binary options to retail clients. It has also imposed restrictions with respect to the selling, marketing and distributing of contracts for differences to retail clients and turbos to retail clients (with respect to turbos, among others a leverage cap for such products with crypto as an underlying is imposed).

Finally, there is increasing attention from the AFM for the role of 'influencers' in promoting certain products or firms.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20. Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Currently, no specific rules or regulations apply that govern the use of distributed ledger technology (DLT) or blockchain, other than Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology, which became applicable on 23 March 2023. This pilot regime lays down uniform requirements for firms that intend to operate a DLT infrastructure. DLT market infrastructures may only admit to trading or recording DLT financial instruments on a distributed ledger.

Firms that intend to operate under this pilot regime need to apply for a permission from the Dutch Authority for the Financial Markets (AFM) as a:

- DLT multilateral trading facility;
- DLT settlement system; or
- DLT trading and settlement system.

The pilot regime will, in any case, apply for a period of three years, after which an evaluation at the EU level will take place.

Generally, the use of DLT is subject to existing regulatory legislation (eg, the Dutch Financial Supervision Act (FSA)) depending on its application in any particular case. DLT is a topic that has led to many questions in the Innovation Hub.

Cryptoassets

21. Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The Dutch Central Bank (DNB) and the AFM have stated that digital currencies do not constitute a financial product (such as e-money or a financial instrument) and do not qualify as legal tender. Therefore, in principle, the FSA does not apply to digital currencies.

However, digital currencies may fall within the scope of the FSA on the basis of activities provided in relation to these currencies. For example, this would be the case when the holder of a digital wallet is able to convert its digital currency holdings into cash holdings held with the crypto-service provider. Further, depending on the structure and the specific characteristics of the digital currency or digital wallet, the relevant services could be considered to constitute payment services or e-money-related services. In these circumstances, unless an exemption applies, the relevant activities trigger a licence requirement under the FSA and certain prudential and conduct-of-business rules will apply.

Additionally, crypto service providers that provide exchange services between virtual and fiat currency or custodian wallet services in or from the Netherlands are required to register with the DNB.

On 24 September 2020, the European Commission published a draft Markets in Crypto-Assets (MiCA) Regulation.

Under the MiCA Regulation, currently, out-of-scope assets and service providers will be regulated. Under the MiCA Regulation, cryptoassets are categorized as e-money tokens, asset-referenced tokens and cryptoassets other than asset-referenced tokens and e-money tokens (including utility tokens). This categorization also covers certain types of stablecoins.

Cryptoassets that are currently regulated (eg, as a financial instrument or e-money) will not fall within the scope of the MiCA Regulation. Also, unique NFTs for now will not fall within the scope of the MiCA Regulation (fractional NFTs and large NFTs collections will fall within scope).

Further, the MiCA Regulation will regulate certain cryptoasset services, including:

- the provision of custody services;

- the operation of a crypto trading platform;
- the exchange of cryptoassets for funds;
- the exchange of cryptoassets for other cryptoassets;
- the execution of client orders in cryptoassets;
- the placing of cryptoassets;
- the reception and transmission of client orders in cryptoassets;
- the provision of advice on cryptoassets;
- the provision of portfolio management on cryptoassets; and
- the provision of transfer services for cryptoassets.

In this context, the MiCA Regulation introduces a licensing requirement for firms providing the above-mentioned cryptoasset services (crypto asset service providers (CASPs)). In addition, the MiCA Regulation introduces the requirement for issuers of certain types of cryptoassets to publish a white paper (setting out the core information on these cryptoassets) and a licensing requirement for issuers of asset-referenced tokens.

On 16 May 2023, the final step of the legislative process was taken by the adoption of the MiCA Regulation by the EU Council. It is the expectation that the MiCA Regulation will be published in the EU Official Journal by July 2023 at the latest, with entry into force 20 days after such publication. The MiCA Regulation will apply to CASPs 18 months following the date of entry into force and to issuers of certain cryptoassets 12 months following the date of entry into force.

Token issuance

22. Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and

other token generation events?

The DNB and the AFM have stated that digital currencies do not constitute a financial product (such as e-money or a financial instrument) and do not qualify as legal tender. Therefore, in principle, the FSA does not apply to digital currencies (unless these in specific circumstances do qualify as financial instruments). However, digital currencies may fall within the scope of the FSA on the basis of activities provided in relation to these currencies.

Further, crypto service providers that provide exchange services between virtual and fiat currency (eg, by operating a crypto exchange) in or from the Netherlands are required to register with the DNB.

Additionally, digital currency exchanges, crypto-brokers and issuers of cryptoassets may fall within the scope of the future MiCA Regulation.

Finally, the AFM warned regarding the serious risks associated with ICOs, such as their vulnerability to misrepresentation, fraud and manipulation, their potential use for the laundering of money obtained by criminal means and the possibility that investors may lose their entire investment. In this context, the AFM advises customers to avoid investing in ICOs.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23. Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Currently, there is no specific regulatory framework for the use of artificial intelligence (AI). Nevertheless, both the Dutch Central Bank (DNB) and the Dutch Authority for the Financial Markets (AFM) pay particular attention to the use of AI. For example, in 2019, the DNB published general principles for the use of AI in the financial sector. The DNB and the AFM focus on the use of AI in the insurance sector, by among others conducting market research.

Further, in its report Machine Learning in Trading Algorithms, published in March 2023, the AFM reminds the market of the risks related to the use of machine learning in proprietary traders' trading algorithms.

Also, on 21 April 2021, the European Commission published a draft Regulation on the use of AI. A draft negotiation mandate was adopted in the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs and Committee on the Internal Market and Consumer Protection on 11 May 2023. The purpose of this Regulation is to lay down rules for the development, marketing and use of AI.

Further, at the moment there is no specific regulation on automated investment advice. However, the AFM has issued guidelines regarding the duty of care of asset managers who offer semi-automatic portfolio management (and investment advice). These guidelines are not legally binding but they do bring clarity for asset managers. The guidelines are aligned with Dutch law, Directive 2014/65/EU (Markets in Financial Instruments Directive II) and suitability guidelines published by the European Securities and Markets Authority and set out, among other things, guidance on safety and the provision of information.

The AFM has published its views on robo-advice more generally, stating that while robo-advice could be an opportunity to improve both access and the quality of investment advice, there are also specific points of attention to consider.

However, on 1 July 2020, the Dutch draft legislation on automated advice was published as part of a publication consultation. This legislation aims to introduce safeguards to ensure adequate provision of automated advice. In this context, the legislation:

- applies competence requirements to automated advice;
- requires that two individuals are responsible for the automated system and advice; and

- imposes rules on controls and systems.

This legislation targets automated advising on financial products in general. On 3 May 2023, the Dutch Council of State issued its advice on this draft legislation.

CHANGE OF CONTROL

Notification and consent

24. Describe any rules relating to notification or consent requirements if a regulated business changes control.

If a qualifying holding (at least 10 percent of the shares or voting rights, or both) is obtained in certain Dutch financial firms (such as settlement institutions, banks, managers of undertakings for collective investment in transferable securities, investment firms, entities for risk acceptance, premium pension institutions, insurers, reinsurers, payment service providers and electronic money institutions), prior approval by the Dutch Central Bank (DNB) is required. In specific cases, increases in qualifying holdings above certain thresholds are also notifiable to or subject to approval from the DNB.

This also applies to any qualifying holdings in Dutch registered crypto service providers.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25. Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

There is no general framework under which fintech companies are required to have in place procedures to combat bribery or money laundering. Nevertheless, financial firms are generally subject to anti-money laundering and combating the financing of terrorism requirements.

Further, as of 21 May 2020, certain crypto service providers fall within scope of the Money Laundering and Terrorist Financing (Prevention) Act.

This concerns companies, legal entities or natural persons that provide:

- services for the exchange between virtual and fiat currencies; and
- services offering custodian wallets (namely, services to safeguard private cryptographic keys on behalf of customers; consequently, 'soft wallets' do not fall within the scope).

These crypto service providers are required to register with the Dutch Central Bank (DNB), to the extent they provide exchange services between virtual and fiat currency or custodian wallet services 'in or from the Netherlands'. A crypto service provider is providing services 'in the Netherlands' if it has directed its activities to the Dutch market (eg, marketing, use of the Dutch language, offering the possibility to pay via Dutch-specific payment methods (such as iDEAL) etc). Non-EEA crypto service providers are currently not eligible for registration with the DNB.

Requirements for such registration include (but are not limited to) having in place an adequate integrity policy to ensure ethical operation management. In this policy, an analysis of integrity risks, compliance with the Dutch Sanctions Act, transaction monitoring, reporting of unusual transactions to the Financial Intelligence Unit-Netherlands and customer due diligence must be covered. Further, the DNB applies a 'wallet verification requirement' in relation to incoming and outgoing transactions in the context of sanctions screening.

Other requirements for registration include, among others, that:

- the policymakers of crypto service providers are trustworthy and suitable; and
- the (directors of) holders of a qualifying holding in (at least 10 percent of the shares or voting rights, or both) and ultimate beneficial owners

of crypto-service providers are trustworthy.

Guidance

26. Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no regulatory or industry anti-financial crime guidance specifically for fintech companies. However, the Dutch Authority for the Financial Markets, the DNB and the Dutch Authority for Consumers and Markets have set up the Innovation Hub to support market operators, such as fintech companies. The purpose of the Innovation Hub is to provide new and existing firms with support in answering queries related to the regulation of innovative financial products and services.

Further, the DNB has published a brochure titled 'Good practices fighting corruption' and the DNB website provides answers to questions regarding the DNB's integrity supervision of crypto-service providers. As regards anti-money laundering and combating the financing of terrorism, the DNB issued a comprehensive guidance in December 2020 titled 'Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Dutch Sanctions Act', which is also relevant for payment service providers, e-money institutions and certain crypto service providers.

DATA PROTECTION AND CYBERSECURITY

Data protection

27. What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The transfer of personal data is subject to local and EU data protection laws (specifically the General Data Protection Regulation (GDPR)). On 25 May 2018, the GDPR came into force with direct effect across the European Union.

It governs the storage, viewing, use of, manipulation and other processing by businesses of data that relates to a living individual. In summary, the GDPR requires that businesses may only process personal data where that processing is done in a lawful, fair and transparent manner, as further described in the GDPR.

The GDPR requires that any processing of personal data must be done pursuant to one of six lawful bases for processing. The most commonly used lawful basis for processing (outside an employment relationship) is the consent of the data subject to that processing. To have obtained valid consent, consent must be freely given, specific, informed, unambiguous and capable of being withdrawn as easily as it is given. Also, it must be made by way of a statement or clear affirmative action. This places a significant burden on businesses to ensure that their customers are fully informed on what their personal data is being used for, which is a crucial change to the previous regime under which disclosure did not need to be so transparent.

Organizations often engage other organizations to process personal data for them. For example, by using a cloud service that stores personal data. Such another organization is called a processor. The organization that engages the processor is the controller. Depending on the location of the processor, specific requirements apply to the transfer of data. If the processor is located in the European Economic Area, the transfer of data is permitted. The requirements of article 28 of the GDPR must be documented. Where a data processor carries out processing on behalf of a data controller, article 28 of the GDPR requires the parties to enter into a written agreement, which imposes specific obligations on the data processor.

If the processor is located outside the European Economic Area and data is transferred outside of the European Economic Area, the GDPR requires the controller to specify the condition relied upon for the international data transfer to ensure that the transferring personal data is afforded the same level of

protection as applies to it in the European Economic Area.

A number of possible safeguards can be taken, such as:

- a transfer to an ‘adequate’ country, which is the simplest way to transfer personal data outside the European Economic Area. This is a formal decision made by the European Union, which recognizes that another country, territory, sector or international organization provides an equivalent level of protection for personal data as exists within the European Union;
- standard contractual clauses approved by the European Commission that can be adopted for the transfer of personal data to controllers and processors located outside of the European Economic Area;
- binding corporate rules; and
- derogations, which can only be relied on in the absence of an adequacy decision for the third country to which the data is to be transferred and derogations are limited to occasional transfers only.

This includes the onward transfers of personal data from a third country or an international organization to another third country or to another international organization (as stated in article 44 of the GDPR).

In the absence of an adequacy decision, or of appropriate safeguards, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only on one of the following conditions (as stated in article 49 of the GDPR):

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; and
- the transfer is made from a register, which according to Union or EU member state law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or EU member state law for consultation are fulfilled in the particular case.

Obtaining consent for non-EEA transfers is a derogation from the rule that data must not be transferred outside the European Economic Area unless the destination country provides an adequate level of protection or an adequate safeguard is in place. As a general principle, the derogation is limited to occasional transfers and is not intended to cover transfers that occur on a regular basis. The explicit consent (namely, an affirmative action) of the data subject, rather than just mere consent must be obtained, and consent must be specific to the transfer. The data subject must also be informed of the possible risks associated with such transfer. Guidance on this notes that if the controller does not have a specific transfer envisaged at the time of collection of the data

it cannot ask for consent at that stage to a possible future transfer but must request it again once the circumstances are known. Further, a request for consent must be brought specifically to the data subject's attention and cannot be concealed or contained within a fair processing notice. This is because the GDPR imposes a high threshold for obtaining consent, namely that consent must be freely given, informed, specific and unambiguous. On this basis, the fair processing notice would not suffice in itself. The level of consent required is even greater than in relation to standard GDPR processing, as data exporters must make additional efforts to make data subjects aware of the risks of transferring to third countries, and therefore would not be a feasible long-term solution.

The laws of the country where the data is transferred will also apply to that personal data when it arrives in that country. The Dutch General Data Protection Regulation (Implementation) Act (UAVG) does not impose any additional requirements on the transfer of data to third countries outside the European Economic Area other than those already listed above.

The GDPR further differs from the previous regime in that it places a significantly increased compliance burden on businesses, including, for example, mandatory requirements to notify regulators of data breaches, obligations to keep detailed records on processing and requirements for most entities to appoint a data protection officer. Businesses that infringe the GDPR may be subject to administrative fines of an amount up to €20 million or 4 percent of global turnover, whichever is higher.

Personal data can be pseudonymized and anonymized. In the first case, personal data is still personal data, in the second case it is not. Recital 26 of the GDPR states that where data has been processed such that it is truly anonymized, the principles within the GDPR do not apply to the processing of that data. When personal data is processed and this data is anonymized, the UAVG no longer applies to that anonymized data. However, the anonymization

of personal data itself does constitute a processing operation to which the UAVG fully applies. Anonymous data means data that cannot be traced back to an identified or identifiable natural person.

The Article 29 Working Party has released Opinion 05/2014 on Anonymization Techniques (in the context of the previous EU data protection regime). This Opinion discusses the main anonymization techniques used – randomization and generalization (including aggregation). The Opinion states that when assessing the robustness of an anonymization technique, it is necessary to consider:

- if it is still possible to single out an individual;
- if it is still possible to link records relating to an individual; and
- if information can be inferred concerning an individual.

In relation to aggregation, the Opinion further states that aggregation techniques should aim to prevent a data subject from being singled out by grouping them with other data subjects. While aggregation will avoid the risk of singling out, it is necessary to be aware that linkability and inferences may still be a risk with aggregation techniques.

The position on anonymization taken from the Article 29 Working Party's Opinion is broadly unchanged in the GDPR. The GDPR itself also gives limited guidance on anonymization in Recital 26, requiring data controllers to consider a number of factors in deciding if personal data has been truly anonymized, including the costs and time required to de-anonymize, the technology available at the time to attempt de-anonymization and further technological developments that may take place.

Further, there are no legal requirements or regulatory guidance relating to personal data that are specifically aimed at fintech companies.

Cybersecurity

28. What cybersecurity regulations or standards apply to fintech businesses?

Directive (EU) 2015/2366 (second Payment Services Directive) (PSD2) includes provisions relating to measures that should be implemented by payment institutions, such as securing the payment service user's personal security data and agreeing on how to manage operational and security risks. Annually, payment service providers must file a report to the Dutch Central Bank (DNB). The report needs to contain an assessment of operational and security risks relating to the payment services provided. In addition, the report needs to address the adequacy of the financial institution's mitigating measures and control measures.

Second, payment service providers must notify the DNB of any major operational or security incidents within four hours after detection. If the incident (possibly) impacts the financials of the users, the payment service must notify them about the incident, without undue delay. Last, the payment service provider must inform users of the measures taken to mitigate the damaging effect of the incident.

In addition to the PSD2, the Security of Network and Information Systems Act requires that certain fintech firms report serious digital security incidents to the National Cyber Security Centre. These are fintech firms that have at least 50 or more employees and (or) generate a revenue of at least €10 million and provide essential services (eg, energy, banking, financial markets infrastructure).

Further, Regulation (EU) 2022/2554 (Digital Operational Resilience Act) (DORA) came into force on 1 January 2023. It aims to harmonize IT regulations for the industry and further strengthen digital resilience. DORA imposes requirements on financial firms with regard to IT risk management, IT incidents, periodic digital resilience testing and risk management when outsourcing to IT service providers. Additionally, arrangements for sharing information on cyber threats have been developed. As of January 2025, DORA

will apply to, among others, financial firms.

Among other things, DORA contains the following requirements:

- firms are expected to have an ICT risk management framework that detects and mitigates risks, and that this risk management is appropriately recorded. Enterprises should also conduct an annual risk assessment and set up business continuity processes.
- firms are expected to manage, classify and handle incidents and significant cyber threats in a process-based manner. It also prescribes, among other things, that regulators should be actively informed about the handling of critical IT incidents.
- firms must have a programme for testing their digital resilience.

Finally, the GDPR includes a few provisions relating to the security of processing, such as the requirement for the controller to, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures that are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing to meet the requirements of the GDPR and protect the rights of data subjects. The controller and the processor must also implement these measures to ensure a level of security appropriate to the risk, which may include, among other things:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the

effectiveness of technical and organizational measures for ensuring the security of the processing.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29. Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Where a financial services company outsources a material aspect of its business, it remains responsible for the outsourced activities. Further, outsourcing must not obstruct supervision by the authorities, and outsourcing by financial firms of critical or important functions must be notified to the regulator.

If a financial service provider plans on using a third party for activities for which a licence is required, this can only be done where both parties have a licence for these activities. For certain activities (such as fund management, investment services, payment services and elements of the CDD process under the Dutch Money Laundering and Terrorist Financing (Prevention) Act) further detailed outsourcing provisions apply.

Cloud computing

30. Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

If a financial institution wants to make use of cloud computing, it must notify the Dutch Central Bank (DNB) of its intention to do so, regardless of the materiality of the outsourced activities. Before using cloud computing, the financial institution is required to develop a risk analysis, which must be presented to the DNB. Because the DNB qualifies cloud computing as a specific type of outsourcing, the rules on outsourcing apply. In addition, the

DNB expects that the EBA recommendations on outsourcing to cloud service providers are taken into consideration.

Outsourcing is not allowed in cases where it would obstruct the supervision of the outsourced activities or where the internal audit function would be negatively affected by the outsourcing of the activities. Further, the financial institution is required to have adequate policies and proper procedures to manage outsourcing risks.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31. Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer programs (and preparatory materials) are protected by copyright. Copyright arises automatically as soon as the computer program is created, registration is not required. Copyrighted works are protected until 70 years after the death of the creator.

Databases underlying software programs may also be protected by copyright and, in certain circumstances, by database right. A database right is a stand-alone right that protects databases that have involved a substantial investment in obtaining, verifying or presenting their contents. The right automatically comes into existence upon creation and expires after 15 years.

Software may also be protected as confidential information or as a trade secret by keeping the software code secret. There are no formal (registration) requirements other than that a trade secret holder needs to take reasonable measures to protect its secret and it needs to have commercial value.

Computer programs and schemes, rules or methods of doing business as such are expressly excluded from patentability under the Dutch Patent Act 1995 and the European Patent Convention. However, patent protection for software may

be possible if the inventor is able to demonstrate that the software makes a novel and inventive technical contribution over and above that provided by the computer program or business method itself. To obtain patent protection, registration is required with the relevant Dutch and European patent offices and the registration requirements must be followed. Patent protection is limited to 20 years starting from the date of filing the application.

IP developed by employees and contractors

32. Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Copyrights and databases created by an employee during the course of his or her employment are automatically owned by the employer unless the parties have agreed otherwise. Patents protecting inventions made by an employee in the course of his or her normal duties are owned by the employer. Any other patented inventions will be owned by the employee unless agreed otherwise.

Inventions or copyrights created by contractors or consultants in the course of their duties are owned by the contractor or consultant unless otherwise agreed. By contrast, database rights are owned by the person who takes the initiative and assumes the risk of investing in obtaining, verifying and presenting the data in question. Depending on the circumstances, this is likely to be the business that has retained the contractor or consultant.

Joint ownership

33. Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Where two or more persons jointly own an intellectual property right, any one of them may use and enforce the right, unless otherwise agreed. Each joint owner may assign or charge its share of the intellectual property right without

the other owners' consent. Exploitation of the intellectual property right, including the granting of licences and charging or assigning the intellectual property right, can only be done by the joint owners of the intellectual property right.

Trade secrets

34. How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

In the Netherlands, trade secrets are protected by the general law of tort (such as breach of the rules of fair competition) and by the Dutch Trade Secrets Act, which entered into force on 23 October 2018 and implements Directive 2016/943/EU (Trade Secrets Directive). The Trade Secrets Act provides more specific rules for the protection of trade secrets. The Trade Secrets Act defines a trade secret as information that:

- is secret, in the sense that it is not generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and
- has been subject to reasonable steps by the holder of the information to keep it secret.

The Trade Secret Act contains measures and remedies to enforce trade secrets. The secret holder can claim an injunction against further use or disclosure of a trade secret. This includes injunctions against infringing goods, which are goods, the design, characteristics, functioning, production process or marketing of which significantly benefit from trade secrets unlawfully acquired, used or disclosed. The Trade Secret Act includes the possibility for the court to grant the winning party a full cost award of all reasonable and equitable legal costs and other costs.

Measures are available in the Netherlands to prevent public disclosure of trade secrets during court procedures. For example, the court may order oral hearings to be conducted 'behind closed doors' and hand down decisions in which confidential information is redacted. The current Trade Secret Act proposal includes a new rule introducing the option for the court to impose a confidentiality club, limiting the access to trade secrets.

Branding

35. What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected as registered trademarks either in the Benelux alone (as a Benelux trademark) or across the European Union (as an EU trademark). Certain branding, such as logos and stylized marks, can also be protected by design rights and may also be protected by copyright. Design rights and trademarks are obtained by registering the design or trademark with the relevant authority (eg, the Benelux Office for Intellectual Property, World Intellectual Property Organization or European Union Intellectual Property Office).

The Benelux and EU trademark databases can be searched to identify registered trademarks or applications for a trademark with effect in the Netherlands. It is highly advisable for new businesses to conduct trademark searches to check whether earlier registrations exist that are identical or similar to their proposed brand names.

Remedies for infringement of IP

36. What remedies are available to individuals or companies whose intellectual property rights have been infringed?

As a preliminary point, on 1 June 2023, the new Unified Patent Court (UPC)

commenced. The UPC offers a single, specialized patent jurisdiction for participating EU member states. The UPC has a court of first instance, which is divided into local divisions. The Netherlands will host one of these local divisions. For European patents that designate the Netherlands and are not opted out of this new system, it is also possible to litigate these in the Dutch local division of the UPC.

For the sake of completeness, we note that the below is meant as a listing of remedies available in the Dutch national courts for IP infringements (although these remedies are also available within the UPC).

Remedies available in the Dutch national courts include:

- preliminary and final injunctions (preliminary injunctions are available cross-border);
- damages or surrender of profits;
- delivery up or destruction of infringing products;
- orders to disclose certain information that relates to the infringement;
- publication orders; and
- reimbursement of costs, including court fees and costs of (patent) attorneys and experts (cost orders in Dutch intellectual property litigation are based on guidelines that provide fee caps for compensation that can be awarded in different types of proceedings. The highest fee cap is for highly complex patent litigation in the first instance, for which the fee cap is €250,000. In special circumstances, the courts may deviate from the fee caps in the guidelines).

COMPETITION

Sector-specific issues

37. Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

The Dutch Authority for Consumers and Markets (ACM) continuously monitors compliance with competition law by companies active in all sectors and also including the financial sector. By means of the Financial Sector Monitor, the ACM carries out economic research into the operation of the financial markets and analyses the risks to competition. In previous years, the ACM presented its findings on competition in this respect. Further, the ACM has specific powers regarding payment system providers and interchange fees.

In 2016, the ACM called for public input on how it can help to boost fintech companies' contribution to competition in the financial sector whereby it indicated it would pay special attention:

- to barriers to entry that prevent the fintech sector from reaching its full potential; and
- to risks involved with rapid technological change that may have adverse effects on competition and innovation.

Following this communication, the ACM has so far looked into the following two specific issues:

- whether regulatory costs constitute barriers to entry for fintech companies. The ACM ordered a study from EY that concluded that such regulatory costs do not constitute obstacles for new providers in the financial sector; and
- whether banks are limiting access of fintech companies – front-end providers and end-to-end providers – to bank accounts and thereby hinder competition in the payment market.

The ACM identified a risk of foreclosure of front-end providers. As a result, the ACM announced that it will actively monitor the behaviour of banks and

how they deal with requests for access. In addition, the ACM:

- proposed that where possible, in light of Directive (EU) 2015/2366 (second Payment Services Directive) (PSD2) and the European Commission's Regulatory Technical Standards, further national implementation of EU law regarding access to bank accounts should enable such access;
- indicated that a system of free access could result in the banks refusing access (which implies that the ACM proposes to allow the banks to ask for compensation for the costs related to providing access); and
- proposed that a light version of the banking licence could be created for fintech companies so that they can offer payment accounts.

As regards end-to-end providers, the ACM considered that the risks of foreclosure were limited. Nevertheless, it proposed to cut the red tape – in addition to the above-mentioned light banking licence:

- by defining objective permit criteria that are related to the actual risks posed by end-to-end providers; and
- by making sure that, in the development of instant payments infrastructures in Europe, fintech companies are able to directly participate in the systems and arrangements for clearing and settlement of payments under non-discriminatory and objective condition.

In 2020, the ACM – on request of the Ministry of Finance – conducted a market study into the role of Big Tech (Amazon, Ant Group, Apple, Facebook, Google and Tencent) in the Dutch payment market and more specifically on the segments counter payments, online payments and payments between consumers. In this study, the ACM concluded that the presence of Big Tech at the time was limited but that it is growing and that Big Tech primarily offered consumers innovative means of payment (citing the use of smartphones for

payment or the recent entry of Apple Pay on the counter payments segment). The ACM expected the presence of Big Tech, as well as the use of such payment methods by consumers, to increase in years to come and noted that these companies choose to offer payment services to reinforce their ecosystems, rather than being driven by the introduction of PSD2.

The ACM identified the following competition risks:

- access restrictions for new innovative players such as Big Tech and fintechs; and
- Big Tech leveraging its dominant market position in neighbouring markets to tip the payment market (through self-preferencing).

The ACM concluded that an amendment of PSD2 may be to ensure that it also applies to Big Tech as gatekeepers to ensure a level playing field for competitors and a free choice for consumers. The ACM in this respect also fully supports the European Commission's Digital Markets Act, which creates various obligations and prohibitions for certain digital services companies (gatekeepers).

In 2021, after having received complaints from dating-app providers, the ACM concluded that Apple abused its dominant position. The ACM determined that if an app provider offers digital content or services within the app for a fee, the app provider is required to agree to additional contractual conditions set by Apple.

These conditions required app providers to use Apple's payment system for the processing of payments and stipulated that app providers are not allowed to refer within their own apps to payment options outside the app, for example, to alternative payment options that app providers offer on their websites. According to the ACM, this constituted an abuse of a dominant position. The ACM, therefore, ordered Apple to change its conditions and imposed an order subject to periodic penalty payments. After incurring the maximum penalty

payment, Apple changed its conditions and now allows different methods of payment in dating apps in the Netherlands. In view of the ACM, Apple now meets the requirements that the ACM sets under EU and Dutch competition rules.

In 2022, the ACM requested the Ministry of Finance to fix a flaw in the national legislation implementing the PSD2. Because of this flaw, the ACM could only take action if a payment institution had been granted a licence by the Dutch Central Bank. The ACM could not handle complaints or reports about banks filed by payment institutions that had been granted licences from other EU regulators. As a result, the ACM was unable to conduct effective oversight over Dutch banks that refuse to offer a bank account to payment institutions, such as fintechs, from other EU countries. To fix this flaw, the national legislation was amended in 2023.

TAX

Incentives

38. Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

Investing in the fintech sector is encouraged by the Dutch government. Two main tax incentives are available for fintech companies and investors in the Netherlands, being of the innovation box regime and the research and development (R&D) wage tax rebate.

Innovation box regime

Dutch taxpayers may claim a particular tax treatment providing for an effective corporate income tax rate of 9 percent instead of the statutory rate of 25.8 percent (2023 rates) on profits realized in respect of certain intangible assets, such as patents, developed by the taxpayer (the innovation box). The regime

applies insofar as the total income from the intangible assets to which the regime applies exceeds the total R&D costs for these assets. Further, the Netherlands applies a nexus approach limiting the benefits of the regime if R&D activities are outsourced to related parties. Software can also qualify as an intangible asset.

Wage tax deduction incentive to invest in R&D

- The R&D tax rebate (wage tax deduction (WBSO)) offers compensation for part of a company's R&D wage costs, other costs, and expenditures. In practice, the WBSO provides for a reduction in payroll taxes to be withheld from the salary of employees engaged in R&D in the Netherlands. As a result, the WBSO decreases a company's personnel costs providing a liquidity benefit to the employer.

- The WBSO amounts to 32 percent of the first €350,000 of R&D wage and other costs and expenses, and 16 percent of all further R&D costs and expenses. For start-ups, the tax deduction for the first €350,000 spent on R&D is 40 percent (2023 rates).

Accelerated deprecation for corporate income tax purposes

In addition to the above-mentioned innovation box regime and the WBSO, special tax incentives are available in the Netherlands to stimulate sustainable entrepreneurship. An investment rebate is a tax incentive in the form of an additional deduction amounting to a certain percentage of the investment made. Currently, there are several investment rebates available in the Netherlands. These investment rebates are:

- the small-scale investment rebate (KIA);

- the energy investment rebate (EIA); and

- the environmental investment rebate (MIA).

With respect to the EIA, an additional extension is provided for the flexible depreciation of qualifying investments (VAMIL).

The KIA is applicable when a maximum of €353,973 (amount for 2023) is invested in any relevant financial year. The KIA is not limited to sustainable investments but is generally applicable. To encourage investments in efficient energy assets, the EIA amounts to 45.5 percent of the investment in 2023. The EIA applies subject to certain conditions. In 2023, the MIA allowance amounts to 45, 36, or 27 percent of the investment amount.

Other than the above-mentioned investment rebates, the VAMIL does not create an additional deduction in the corporate income tax return, but provides for a temporary difference by allowing accelerated depreciation on assets in one year up to a maximum of 75 percent. The remaining 25 percent is depreciated on a straight-line basis.

Tax treatment of stock options

As of 1 January 2023, the tax treatment of employee stock options has changed as per that date the taxable moment for payroll withholding tax purposes due on stock options on (non-tradable) shares awarded to employees is deferred to the moment the shares become tradable. This change was introduced to attract and retain employees and make the Netherlands more competitive for start-ups and scale-ups providing by providing a (temporary) liquidity benefit. However, at the employee's discretion, taxation can still take place at the moment of exercise of the stock option as was the case under the old legislation.

Before implementation of the legislative proposal, payroll withholding taxes were to be withheld if an employer granted stock options to an employee at the moment when the employee exercised or sold the stock option. The taxable base consisted of the fair market value of the stock option at that moment. Due to the legislative change, the taxable moment for payroll withholding tax purposes is by default deferred to the moment the shares become tradable

unless the employee opts for taxation at exercise. In the latter situation, any increases in value after the moment of taxation will not be subject to wage tax, and any benefits derived, most notably dividends, are not taxable as wages.

Increased tax burden

39. Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

Directive on a minimum effective tax rate of 15 percent

Pillar 2, an initiative by the OECD/G20 Inclusive Framework, introduces a minimum level of taxation for multinationals with an annual consolidated revenue of at least €750 million. In scope, multinationals will at all times pay a minimum effective tax rate of 15 percent on their worldwide profits, whereby their tax base is determined by reference to a multinational enterprise's financial accounts income after certain tax adjustments have been applied.

The European Commission published a directive proposal along the lines of the OECD Pillar 2 proposal. Adoption of the directive proposal requires a unanimous decision from all EU member states. Directive (EU) 2022/2523 (Pillar 2 Directive) was published in the Official Journal of the European Union on 22 December 2022. Currently, the intention is that EU member states need to implement the Pillar 2 Directive by 31 December 2023. On 24 October 2022, the Dutch legislator published a draft legislative proposal for the implementation of Pillar 2 and will prepare a final legislative proposal, to be submitted for approval to the Dutch parliament.

Under Pillar 2, a top-up tax should typically be due if the effective tax rate of the multinational enterprise group is lower than the minimum tax rate of 15 percent. The primary mechanism for the implementation of Pillar 2 will be an income inclusion rule (IIR) pursuant to which additional top-up taxes are payable by a parent entity of a group if one or more constituent members of the

group have been undertaxed. A secondary fall-back is provided by an undertaxed payment rule (UPR) if the IIR has not been applied. The UPR can be applied by:

1. limiting or denying a deduction for payments made to related parties; or

2. making an adjustment in the form of an additional tax.

In the Dutch draft legislative proposal published on 24 October 2022, the Netherlands opted for option (2).

Thirty percent facility for expats capped at WNT standard

Under the 30 percent facility, certain employees recruited from abroad to work in the Netherlands can receive a maximum of 30 percent of their wages tax-free. The Dutch government plans to cap the 30 percent facility as of 1 January 2024 for expats at the WNT standard (the maximum allowed income in the public-service sector). In 2023, this standard was set at an income of €223,000 per annum. Transitional rules may apply.

IMMIGRATION

Sector-specific schemes

40. What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

The following are the most common corporate immigration schemes in the Netherlands (only relevant for non-EU, EEA and Swiss nationals – third-country nationals – since all EU, EEA and Swiss nationals are free to reside and perform any activities in the Netherlands as long as they wish since there is free movement of workers within the European Union, which is expanded to the EEA and Switzerland).

- Knowledge migrant scheme (highly skilled migrant scheme): this has nothing to do with knowledge as such, but everything with the gross monthly salary (exclusive of holiday allowance, normally 8 percent of the salary) that is consistent with Dutch salary standards and with thresholds for 2023 that vary from €2,631 to €5,008 per month, depending on age or graduation date in the past three years before applying for such a residence permit from a Dutch or top 200 university from a master's degree or PhD (if graduation is from a university in the Netherlands then bachelor level is also allowed). In addition, the offered salary needs to conform with the prevailing market (namely, normal for the job title). These salary thresholds are indexed each year. However, this does not mean that the salary of the employee needs to change every year. In principle, changes need to be made when the validity of a residence permit is extended, the employee changes employer or the employee changes the purpose of the residence permit. In addition to the aforementioned, the formal employer in most cases needs to hold the status of a recognized sponsor for the purpose of regular labour and knowledge migrants. If the employer is not a recognized sponsor, the employer can apply for that or make use of a payroll company that is a recognized sponsor. The formal employer would borrow their recognized sponsorship, in which case the payroll company would be the formal employer and second the employee to the factual employer. The employer is also able to become a recognized sponsor by submitting an application to the Immigration and Naturalization Service (IND); as a result, the employer will be considered a reliable partner of the IND.

- Intra-corporate transfer scheme (Directive 2014/66/EU (Intra-Corporate Transit Directive)): if the employee is a specialist, manager or trainee and remains on the payroll of his or her employer outside the European Union, and the employee was already employed

at that entity outside the European Union within the same group of companies, he or she may be transferred to the Netherlands under the intra-corporate transfer scheme for up to three years for a specialist or a manager and for up to one year for a trainee (after which he or she can return to the country from where he or she was seconded, or the residence permit can be changed into, eg, a residence permit as a knowledge migrant provided that the salary criterion is met and the employer is a recognized sponsor). The validity of a residence permit as an intra-corporate transferee cannot be extended if, with that extension, the maximum duration of one (trainee) or three (specialist or manager) years is exceeded). No salary thresholds are applicable but the salary criterion for knowledge migrants is an indication, albeit that the salary needs to conform with the prevailing market and, of course, complies with the Dutch minimum wage Act. Also, no recognized sponsorship is required, but is nevertheless advisable for a faster procedure. As a recognized sponsor, the application procedure should just take two weeks instead of 90 days. Some form of intra-EU mobility is possible for a long or a short term, which for a short term would not lead to needing another work permit in the other EU country where the employee is temporarily transferred within the same group of companies. This scheme takes precedence over other schemes if the application or situation falls within the scope of the directive. There is also a national intra-corporate transfer scheme; however, with this Directive and the national knowledge migrant scheme, the national intra-corporate transfer scheme is not used that often as there are more requirements to be met.

- EU Blue Card scheme (Directive 2009/50/EC (Blue Card Directive): the EU version of the Dutch knowledge migrant scheme but with a higher salary threshold, and where specific education requirements apply. Foreign degrees must be rated by Nuffic. The salary threshold in

the Netherlands is €5,867 gross per month, exclusive of holiday allowance for 2023. This salary threshold is indexed each year. Recognized sponsorship is not required but is nevertheless advisable due to the more rapid application procedure. The EU Blue Card can be issued for a maximum of four years (depending on the duration of the employment agreement but the employment agreement needs to be for at least one year). After this period, it is possible to renew the EU Blue Card, provided the conditions are met. This scheme remains unpopular in the Netherlands due to the much more flexible national knowledge migrant scheme. The Blue Card does have one advantage: if an employee has a Blue Card that is valid for at least 18 months in another EU country, that employee is already allowed to start working in the Netherlands under the condition that within one month of arrival in the Netherlands, a Dutch EU Blue Card is applied for and in some situations, a permanent residence permit can be applied for earlier than five years.

- International trade regulation: a scheme that may come in handy in certain situations where larger and mostly lower-paid groups of third-country nationals have to come to the Netherlands in the framework of a certain project that has been assessed and approved by the Dutch Employee Insurance Agency (UWV). The salary threshold is the Dutch statutory minimum wage, that on 1 July 2023 increased to €1,995 gross per month, exclusive of an 8 percent holiday allowance. To qualify for the international trade regulation, there must be a time-defined trajectory of initially a maximum of three years, and there must be a relationship between the company in the Netherlands and abroad. The workers (employees, clients or director-major shareholders) must come to the Netherlands to perform specialist or managerial duties. The work done may not be of a competitive nature (priority labour supply). This is assessed, among other things, on the

basis of the nature, duration and value of the trajectory and nature of the work. Once the trajectory has been approved, the workforce only needs to be notified via a form of the UWV, and the workforce can start work immediately. No recognized sponsorship is necessary.

- Short-term knowledge migrant scheme: this has the same salary criteria as the above-mentioned criteria for the knowledge migrant scheme, but varying from €3, 672 to €5,008 gross per month exclusive of holiday allowance and the job in the Netherlands must be a specialist, key, scientific or managerial position. A work permit as a short-term knowledge migrant can be applied for by the employer at the UWV, the recognized sponsor, for short-term assignments for a maximum duration of three out of six months, limited by the duration of the Schengen visa or the free-term requirements of a maximum of 90 out of 180 days.
- The delivery of goods including assembling, repairing, installing, amending and instructing on the use of those goods, which includes software. This is an exemption in Dutch migration law. No work permit is needed for such work if that work is regarded as incidental labour. In this regard, incidental labour means that the work that needs to be done does not take longer than 12 consecutive weeks within 36 weeks. There is no specific salary criterion, but a salary must be consistent with Dutch salaries for similar work. Should the work, however, not fall within the scope of this exemption, there is also a single permit (that combines a work and residence permit) for the assembly and repair of equipment supplied by foreign companies. The personnel costs must, in that case, not be higher than the to-be-delivered goods, the work must not exceed a period of one year and the workers would need to have specific knowledge to finalize the delivery of the goods for the customer to be able to use the goods. In addition, the following activities are also excluded from the obligation for a work permit,

(incidental labour): holding business meetings or concluding agreements with companies and institutions for a maximum period of 13 weeks within a 52-week period and receiving training for a maximum of 12 consecutive weeks within a 36-week period. Note that if the person concerned is going to work, a work permit must be applied for at the UWV, such as a work permit for a knowledge migrant short stay (the short-term knowledge migrant scheme).

- Researcher (Directive 2016/801/EU (Students and Researchers Directive): mostly for researchers and scientists working at universities and other research institutions and companies. A specifically recognized sponsorship is necessary for the purpose of educational institutions. The researcher will work as either a paid researcher, an unpaid researcher with a grant or a PhD candidate and complies with the admittance requirements. Other specific requirements are applicable. The researcher must have at least €1,354.08 gross per month exclusive of holiday allowance as income (salary, scholarship or grant, or in his or her bank account) to comply with the sufficient means of subsistence requirement.

- Intra-EU service provision: exempted from the work permit obligation in the Netherlands if intra-EU service provision is performed under articles 56 and 57 of the Treaty on the Functioning of the European Union, meaning that the work of third-country nationals in the Netherlands by a company based in an EU member state is allowed to provide services to companies in the Netherlands. Note that this is only allowed if the third-country nationals are also allowed to conduct similar work in the country of residence. A residence permit obligation in the Netherlands applies after 90 out of 180 days for the third-country national. Based on the third-country national’s residence permit issued by the authorization of another EU member state, this person can stay for 90 out of 180 days in the Netherlands. At day 91, a Dutch residence

permit as a cross-border service provider is required. This residence permit at this moment has a maximum duration of two years. This is specifically for third-country nationals living and working legally in EU member state A who temporarily perform services or work for their employer in member state B. No salary threshold applies and no recognized sponsorship is needed. Alongside this, as of 1 March 2020, all cross-border service providers need to notify all their employees (including EU, EEA and Swiss nationals) via www.postedworkers.nl before starting to provide services in the Netherlands. Failure to notify on time will lead to a fine.

- Several specific training and trainee schemes. These are the most common schemes for corporate migration out of approximately 40 schemes available in the Netherlands, some based on EU law, some purely based on national law. Every case needs to be assessed by an immigration specialist on an individual basis since a different scheme to those stated above might be better suited. Further, there are several short-term work permit exemptions (incidental labour in the Netherlands), for example, for business meetings, receiving training courses or instructions regarding the use of goods manufactured in the Netherlands and services to be provided in the Netherlands. Living legally in the Netherlands is different from working legally in the Netherlands. It is, in principle, forbidden for a third-country national to perform any work in the Netherlands without a work permit, a work permit exemption or a Dutch residence permit with the suitable labour market annotation or single permit, except for very specific exemptions. Sanctions in the case of non-compliance are high – normally an €8,000 fine per illegally working foreigner and per employer in the meaning of the Dutch Foreigners Employment Act – but in most cases of an administrative rather than a criminal nature, additional sanctions may apply including shutting down the business

operation in the Netherlands by up to three months.

Since 1 January 2021, UK nationals also need to fulfil the same criteria as any other non-EU, non-EEA citizen or non-Swiss national, as they have become third-country nationals.

UPDATE AND TRENDS

Current developments

41. Are there any other current developments or emerging trends to note?

EU developments

Significant current developments relating to fintech seem to be driven at the EU level as a result of EU member states' adoption of the Digital Finance Package in September 2020.

Among other things, the Digital Finance Package introduces the MiCA Regulation (adopted by the EU Council on 16 May 2023, the Regulation is a pilot regime for infrastructure based on distributed ledger technology (which became applicable on 23 March 2023), and Regulation (EU) 2022/2554 (Digital Operational Resilience Act), which will apply as of January 2025). Further, the European Commission published a draft Regulation on the use of artificial intelligence in April 2021 (in respect of which a draft negotiation mandate was adopted by the EU Parliament's relevant Committee on 11 May 2023) and its anti-money laundering and combating the financing of terrorism (AML/CFT) Reform Package in July 2021. The latter will have a significant impact on crypto service providers as it among others brings crypto transfers into the scope of the EU Transfer of Funds Regulation (as endorsed by the EU Council on 16 May 2023) and introduces an EU Regulation on AML/CFT requirements.

Additionally, on 1 June 2023, the Unified Patent Court (UPC) commenced. The

UPC is the most significant change in European patent law in 50 years. It offers a single, specialized patent jurisdiction for participating EU member states. It enables patentees to enforce all designations of a European patent in one single enforcement action at the UPC.

With the UPC, patentees also have the option of applying for unitary patents, which will have effect across all participating EU member states. So far, 17 EU member states have ratified the necessary legislation, and 24 are currently signatory states. Signatory states that have not ratified yet can do so at any time. The unitary patent may provide significant cost advantages and a significant reduction of administrative burdens for patentees that normally validate their patents in multiple EU countries.

Finally, in 2022, both the Digital Services Act (DSA) and the Digital Markets Act (DMA) entered into force, which are also relevant for fintech companies. The DSA imposes multiple obligations (most notably transparency and terms of service requirements) on online service providers, including platforms, whereas the DMA creates various obligations and prohibitions for certain digital services companies (gatekeepers). It is unlikely that a fintech company will be designated as a company falling under the DMA or DSA. However, fintech companies, as beneficiaries of these acts, can enforce compliance with obligations by their service providers, such as access to data.

Dutch developments

On 13 October 2021, the Dutch Minister of Finance published a report on the progress of the implementation of its national Fintech Action Plan. Key items highlighted in this Action Plan include:

- the development of legislation targeting automatic advice;
- increasing the attention for appropriate fees for new entrants (including fintech start-ups); and

- the statement that Dutch fintech companies should not be subject to stricter requirements than necessary.

The European Commission published a directive proposal along the lines of the OECD Pillar 2 proposal. Adoption of the directive proposal requires a unanimous decision from all EU member states. Directive (EU) 2022/2523 (Pillar 2 Directive) was published in the Official Journal of the European Union on 22 December 2022. Currently, it is intended that EU member states need to implement the Pillar 2 Directive into their national laws by 31 December 2023.

On 24 October 2022, the Dutch legislator published a draft legislative proposal for the implementation of the Pillar 2 Directive and will prepare a final legislative proposal to be submitted to the Dutch parliament.

**** The information in this chapter was accurate as of June 2023.***