International
Comparative
Legal Guides

Practical cross-border insights into fintech law

Fintech 2022

Sixth Edition

Contributing Editors:
Rob Sumroy and Ben Kingsley
Slaughter and May

ICLG.com

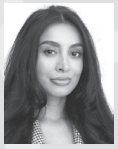
Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

Netherlands

Else Loop-Rowel



Anjali Kaur Doal

De Brauw Blackstone Westbroek

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and the state of the development of the market, including in response to the COVID-19 pandemic and ESG (Environmental, Social and Governance) objectives. Are there any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications)?

The Netherlands has long been recognised as a global front-runner in fintech. It is host to Money 20/20 Europe, Europe's largest and most important fintech event, and Bloomberg's 2021 Innovation Index ranked the Netherlands as the world's ninth most innovative country.

Dutch fintech climate

The Netherlands has a strong business climate for fintechs, with its digital infrastructure, world-renowned culture, fluency in English, and central geographical location being key factors. There are several thriving hubs throughout the Netherlands, including Amsterdam (financial sector), Rotterdam (international trade), and Delft and Eindhoven (technical universities), which together contribute to the Netherlands' thriving fintech climate. The Netherlands is also home to "traditional" fintech businesses (payments, asset management, credit provision, etc.) – with payment unicorns Adyen and Mollie being prime examples – as well as more specialised forms of financial innovators, operating under buzzing common denominators, such as InsurTech, BigTech, PensionTech, LegalTech and RegTech. Many international fintech investors are also active in the Netherlands and there remains a strong influx of investors. The Amsterdam Stock Exchange is gaining popularity and includes three of the largest European tech companies (Prosus, Adyen, and Just Eat Takeaway). Finally, the Dutch government issued an action plan to further advance innovation in the financial sector and enable fintechs to position themselves and further develop in the Netherlands with sufficient capital, knowledge and talent.

Notable trends

Notable recent trends and developments that we see are:

- rapidly increasing investor focus on cryptocurrencies, crypto tokens, and decentralised ledger technology, such as non-fungible tokens (NFTs), increasing attention and use of distributed ledger technology/blockchain to deliver financial services, and an overall trend to shift towards decentralised finance (DeFi);
- increasing regulatory expectations with regards to the use of artificial intelligence (AI);
- increasing attention towards the environmental, social and governance (ESG) aspects of fintech; and
- enforcing the General Data Protection Regulation (GDPR).

In general, we see the fintech environment becoming more mature and professional. As new business models prove successful, more capital, time and effort flow into fintech entities and financial institutions. Examples abound. Banks use technology to advance their business model and Tikkie was the first app in the Netherlands allowing consumers to send instant payment requests. Dutch regulators and decision-makers have generally welcomed fintech businesses, and have tried to facilitate the creation of fintech initiatives as much as possible. As the fintech environment matures, regulations are likely to play a bigger role in the foreseeable future, legitimising these developments even more and strengthening the fintech ecosystem.

Brexit – EU market access

In the aftermath of Brexit, we have seen a significant increase in the number of requests for assistance with EU market access from UK-based fintechs that had previously relied on the EU passport regime to conduct regulated activities across Europe. From our discussions with fintechs seeking EU market access, we understand that they are often attracted to the Netherlands for its:

- broad and developed fintech communities and access to talent;
- approachable and reputable supervisory agencies that are accustomed to communicating in English;
- high-quality digital infrastructure and high adoption rate of innovative technologies; and
- attractive business climate, including the availability of specific tax incentives available to fintechs.

COVID-19 – Digitalisation

COVID-19 has brought the role of technology to the forefront of the financial sector. Even before the crisis, the Netherlands was one of the leaders in European and global lists of digital payments. The COVID-19 pandemic led to an even bigger push towards more cashless payments, online banking, electronic transactions and services, and a general increase in digitalisation of products and services.

Digital euro (Central Bank Digital Currency (CBDC))

As regards non-cash payments, there is already considerable public attention being paid to CBDC in the Netherlands due to the evolving digitalisation throughout the country. After the Dutch government requested the Dutch Central Bank (DNB) to

research CBDC, DNB produced a working paper and comprehensive report on the initial exploratory phase of a digital euro. DNB also contributed to an exploratory international study of the Bank for International Settlements for the same. DNB has explicitly expressed that it has a favourable attitude to CBDC and that it is ready to play a leading role in experimenting with its use, and to contributing to the policy debate. Over the next two years, DNB will be exploring exactly what a digital euro should look like.

ESG

We have seen greater focus on ESG across the financial sector. This also holds true for fintech in particular. The intersection between fintech and ESG leads to challenging considerations, including: cultural and ethical issues raised by products utilising personal data or AI; impact on people and human rights by the use of robots; diversity and inclusion in fintech firms; social inclusion effect of fintech; Bitcoin's carbon impact; the accountability of fintech firms in terms of ESG aspects, etc. In our practice, we generally see an intense focus on governance of financial institutions. We expect that fintechs, especially when using AI, will need to ensure appropriate governance, including, for example, responsibilities and product approval processes, and documented procedures and frameworks.

We also see a big shift underway for fintech start-ups bringing impact investing platforms for more sustainable investment options into the mainstream (Carbon Equity, Startgreen Capital and Oneplanetcrowd, to name a few Dutch companies focusing on climate impact investments).

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction (for example cryptocurrency-based businesses)?

While there are no specific rules that ban or restrict fintech businesses in the Netherlands, the financial services sector is heavily regulated. This means that where fintech businesses offer a financial product or service, such as offering consumer credit or payment services, they need to comply with the financial regulatory laws and regulations that apply to conventional financial institutions, even if the business is more "tech" than "fin". However, DNB has indicated that there is room for the proportional application of legislation and supervision, and has mentioned that the fintech sector would benefit from this approach. Both DNB and the Dutch Authority for the Financial Markets (AFM) have recognised that new fintech solutions do not always fit within existing rules. In our experience, both regulators have an open and constructive attitude towards innovation and, within the limits of their mandate, interpret obligations for fintechs proportionate to their size and complexity.

With regard to cryptocurrency-based businesses, there is a "ban" on providing crypto services in the Netherlands for business that have not registered with DNB (more about this at question 3.2). And where the service provider is registered, only the services that *are registered* can be provided. DNB monitors crypto service providers based on the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act. DNB may exercise its supervisory and enforcement powers in the event of non-compliance, such as an instruction, order subject to a penalty, or a fine. Also, failure to register qualifies as an economic offence under the Dutch Economic Offences Act, based on which DNB can report this information to the Public Prosecutor's office. This may result in criminal prosecution for the persons involved in the cryptocurrency-based business.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

While small and growing fintech businesses are less likely to have access to traditional bank financing or to the capital markets through an IPO or bond issuance, venture/seed capital firms are active in the Dutch market for early-stage financing. The funding rounds by Mollie are a good example of venture capital in fintech. We have noticed that founders want to stay in control of their business, and that they often bring additional capital and/or additional expertise to take them to the next level. Alternatively, the European Investment Bank, backed by the European Fund for Strategic Investments, is regularly considered a funding source. We have also seen fintech businesses choosing to partner with existing financial institutions to finance their operational and development costs, or financial institutions investing in fintechs. Crowdfunding is less common in the Netherlands but is growing in popularity as an additional source of finance.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

From a tax perspective, the Netherlands is an attractive hub for investing in or for expanding fintech businesses in Europe. This is also driven by various tax incentives available to fintech businesses, such as:

Innovation box

If certain conditions are met, the innovation box regime provides that qualifying profits derived from certain qualifying self-developed intangibles (for example, software) are taxed at an effective corporate income tax rate of 9% in 2022.

R&D tax credit

The WBSO (R&D tax credit) of the Ministry of Economic Affairs is intended to provide an incentive to businesses to invest in research. If certain conditions are met, the R&D tax credit provides a tax break for wages tax and national insurance contributions due by employers for wages paid to employees conducting R&D activities in the Netherlands.

Income tax reduction for qualifying expats (the 30% ruling)

Qualifying expats in the Netherlands are entitled to a substantial income tax exemption of up to 30% for a maximum period of five years, resulting in the remaining 70% being subject to income tax.

Reduced corporate income tax rate for small companies

In 2022, the Dutch corporate income tax rate was reduced to 15% for profits up to EUR 395,000. Profits in excess of EUR 395,000 are taxed at 25.8%.

Depreciation of R&D costs

In a departure from general asset depreciation principles, the R&D costs of intangible assets may sometimes be depreciated only once – in the fiscal year where these R&D costs were incurred.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

Before listing securities on a Dutch regulated market, Dutch regulatory law requires businesses to prepare a prospectus, the content of which is governed by European rules, and must be approved by the AFM. For businesses incorporated under the law of another EU/EEA Member State, the approval granting authority is, in principle, the home state regulator. These businesses may "passport" their approved prospectuses into the Netherlands. Subject to certain equivalency standards, the AFM will allow businesses incorporated under the law of a non-EU/EEA Member State to use a non-EU prospectus, in order to acquire a listing on the Dutch regulated market.

Furthermore, a business will need to comply with several laws and regulations, particularly:

- relevant corporate law (for example, the business will need to have a corporate structure in place that allows shares to be freely transferable and tradeable);
- regulations of the local regulated market. However, unlike some regulated markets, Euronext Amsterdam does not have substantive ongoing requirements. For Dutch businesses, "comply or explain" governance recommendations apply, pursuant to the Dutch Corporate Governance Code; and
- ongoing requirements, such as the EU market abuse and transparency rules (disclosure of inside information; notification requirements for shareholders; and disclosure of trades by certain key insiders).

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

The Netherlands has become one of the main global fintech hubs, with a significant increase of fintechs settling here due to the attractive Dutch business climate. For example, the IPO of Adyen in 2018 was the largest public offering on Euronext Amsterdam in years. Since then, we have noticed a trend in the Dutch fintech sector to collaborate with venture capital firms or to partner up with incumbents in order to facilitate further growth instead of selling a fintech business in its entirety. We have also seen examples of fintech founders looking to exit when the business is a bit more mature. For example, Buckaroo, the Dutch leading payment services company, was sold to private equity firm BlackFin Capital Partners.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

The Dutch financial regulatory framework is rooted mostly in European legislation, making it similar to the frameworks of other EU Member States. Regulated activities include conducting banking or insurance (intermediary) activities, and providing payment services. No distinction is made between fintech businesses and incumbents. Whether a fintech business falls within the scope of financial regulation depends on the specific activities it intends to conduct and whether those activities are regulated within the financial regulatory framework.

DNB and the AFM supervise authorised financial institutions in the Netherlands in tandem. While DNB focuses primarily on financial soundness, the AFM supervises market conduct. Both supervisors work closely together where needed.

In the case of cross-border services provision from an EU Member State into the Netherlands, the principle of "home state control" generally applies, meaning that the regulator of an undertaking's home state remains its main regulator. Being active in multiple countries could, however, lead to additional regulatory requirements, as local requirements may also have to be complied with in the host state. This is generally minimal, given the maximum harmonisation aimed for at a European level. Where more than one regulator has supervisory power over an institution, as in the case of multinational banking or insurance groups, the relevant sectoral legislation stipulates which regulator is the main regulator.

3.2 Is there any regulation in your jurisdiction specifically directed at cryptocurrencies or cryptoassets?

The European Revised Fourth Anti-Money Laundering Directive (commonly referred to as the Fifth Anti-Money Laundering Directive or AMLD5) provides rules for firms offering services for the exchange between virtual and fiat currencies, and for providers of custodian wallets for virtual currencies. The act implementing the AMLD5 in the Dutch Anti-money laundering and terrorism financing (prevention) Act (*Wet ter voorkoming van witwassen en financiering van terrorisme*, Wwft) entered into force in May 2020. If such crypto service providers are active in a professional/commercial capacity in or from the Netherlands, they must register with DNB. Providers of crypto-to-crypto exchange services do not need to register. The application for registration focuses on: (i) the business plan; (ii) the identity of the board members and shareholders who own a qualifying holding (shares representing 10% or more of shares and/or voting rights); (iii) governance; (iv) sound operational management; and (v) ethical business operations. Registered providers are monitored on an ongoing basis. It is good to note that for fintech businesses, an acquisition of 10% or more of the shares and/or voting rights in a crypto service provider requires DNB's prior approval.

The obligation to register with DNB for crypto service providers offering exchange services between virtual and fiat currencies or custodian wallets in the Netherlands means that crypto service providers located in other EU Member States are also subject to this registration obligation if they provide their services on a cross-border basis to clients located in the Netherlands, regardless of registration in their home state. Furthermore, crypto service providers located in a third country (a non-EU Member State) are prohibited from offering exchange services between virtual and fiat currencies or custodian wallets in the Netherlands.

In July 2021, the European Commission developed a package of legislative proposals intended to strengthen the AML/CFT rules, which would introduce a new EU anti-money laundering authority (AMLA) to improve the detection of suspicious activity and address the loopholes that criminals use to transform illegal funds. The Dutch government is exploring whether the Netherlands could serve as a location for the AMLA. The establishment of the EU AMLA reflects the changing global risk landscape, including the emergence of disruptive fintech start-ups, new payment methods, and virtual currencies.

In addition to the AML rules, crypto service providers must comply with the requirements set out in the Dutch Sanction Act (*Sanctiewet 1977*). The Dutch Sanction Act is a framework act enabling general administrative orders to be issued in compliance with treaties or international agreements on international sanctions imposed by the UN Security Council, the European

Union or national governments. The Netherlands may also independently designate natural persons or legal entities and order their assets to be frozen or the provision of financial services on their behalf to be prohibited or restricted. Such orders are included in, for example, the Sanctions Regulations on Terrorism 2007 and 2007-II (*Sanctieregelingen terrorisme 2007 en 2007-II*). While the Dutch Sanction Act has to be observed by all natural persons and legal entities residing in the Netherlands, crypto service providers would do well to realise that this has a profound impact on their ongoing client monitoring requirement. In recent guidance, DNB indicated that crypto service providers should be able to determine whether a "relationship" produces a hit based on the Dutch Sanction Act or its underlying regulations. In this context, a "relationship" is defined as "anyone involved in a financial service or a financial transaction". This includes the counterparty or other party involved in a transaction by a crypto service provider's client. As such, a crypto service provider has to be able to effectively: (i) establish the identity and place of residence of the counterparty and screen it against the sanctions lists; and (ii) establish that this person or legal entity is actually the recipient or the sender.

Providers of crypto services will become subject to further regulation once the EU Markets in Crypto-Assets Regulation (MiCA) enters into force (directly applicable in the Netherlands), which is expected to take place in 2024. The Dutch government and supervisory authorities have already expressed their desire to further regulate crypto service providers via European legislation. The new framework, currently still in the preparatory stage, would impose a licence requirement on the providers rather than the current *registration* requirement. There will be other requirements touching on market conduct and consumer protection; for example, an obligation for crypto-issuers to provide a prospectus-like "white paper" for the purpose of informing consumers. Under MiCA, there will be more businesses subject to the regulatory framework than is currently the case.

DNB, together with the European Central Bank (ECB) and other European central banks, has investigated the possibilities and possible advantages of issuing CBDC, amongst other reasons in order to be able to offer consumers a reliable alternative to cryptocurrency, while potentially making using of the same underlying technologies. The ECB and central banks are currently working on an analysis of the potential design of such a CBDC, which they intend to finalise in October 2023.

3.3 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested? Are there any regulatory 'sandbox' options for fintechs in your jurisdiction?

In general, Dutch financial regulators and the Dutch government have been receptive to new, innovative technologies and developments in the financial sector. The Netherlands is also one of the few EU Member States to have an innovation hub and a regulatory sandbox.

The Dutch InnovationHub for the financial sector was established in 2016 by DNB and the AFM. The InnovationHub supports businesses that seek to implement innovative financial business models or products, but are unsure about the specific relevant rules. The InnovationHub offers new businesses and incumbents the opportunity to submit questions about supervision and regulations directly to DNB, the AFM or the Dutch Authority for Consumers & Markets, regardless of whether they are subject to a regulatory framework.

DNB and the AFM created a regulatory sandbox to further facilitate innovation and to enable businesses to launch their innovative financial products without unnecessary regulatory hindrance. Applicants can request that the relevant regulator assess whether innovative concepts comply with the underlying purposes of applicable financial markets regulations rather than adhering to a strict interpretation of the law. This enables and encourages any business wishing to launch an innovative financial concept to enter into a constructive dialogue with its regulator. The regulatory sandbox does not explicitly provide a controlled business environment to test products and is open to start-ups and established financial companies active in the Netherlands.

Following the success of the InnovationHub and the regulatory sandbox, DNB established an innovation forum (iForum). The iForum is designed as a platform for joint initiatives that create value for both supervised institutions – such as banks, insurers and pension funds – and DNB. DNB aims to create value by establishing an ongoing dialogue on the impact of technological innovations in the sector, and by developing joint pilots and experiments in areas where technology and supervision meet. For example, DNB investigates the impact of the use of AI in the sector and in supervision; for example, to analyse supervisory data to better understand the opportunities and risks of technological innovation.

3.4 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

Offering financial services or financial products in the Netherlands that fall within the scope of Dutch financial regulatory law, including, for example, payment services and consumer credit provision, in principle, requires prior authorisation by the relevant Dutch regulator. For certain EU-wide regulated types of financial services and products, fintech businesses outside the Netherlands may make use of their authorisation in another EU Member State, which limits the requirements to offer products or services in the Netherlands to a notification procedure only ("passporting"). The Dutch market can then be accessed through a branch or simply via the cross-border provision of services. Payment service providers can also make use of a network of agents to provide cross-border services.

For some financial services the Dutch regulators accept reverse solicitation. In this context, regulators apply the "initiative test": if the services provided to customers in the Netherlands by a business with corporate seat outside the Netherlands are provided *solely at the initiative of the client*, no requirement to obtain prior authorisation from a Dutch regulator applies. However, marketing or advertising activities in the Netherlands, such as providing an option to display the company website in Dutch, could quite easily frustrate the outcome of the initiative test.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The processing of personal data in the Netherlands is regulated by the GDPR, which applies directly in all EU Member States. The Dutch GDPR Implementation Act clarifies, within the limits allowed by the GDPR, the application of the GDPR legal framework in the Netherlands.

The GDPR applies to companies that determine the purpose and the means of processing personal data (controllers), and to companies that process personal data on behalf of the data controllers (processors), such as cloud service providers. The GDPR also introduced rules for joint controllers. Joint controllership takes place when more than one actor is responsible for personal data processing. Defining the roles of controller, processor and joint controller in fintech businesses can be especially challenging, but is important as it is directly linked to enforcement risks, liability and litigation exposure.

The GDPR adopts a principle-based approach to personal data protection. The general principles that must always be observed require that companies:

(i) process personal data lawfully, fairly and in a transparent manner;
(ii) collect personal data only for specified, explicitly defined and legitimate purposes;
(iii) process and store personal data no longer than required for the purpose of the processing; and
(iv) adopt and maintain appropriate measures to ensure the security of personal data.

Along with the GDPR, the second Payment Services Directive (PSD2) regulates the processing of personal data within the framework of payment services. PSD2 requires that banks grant third-party payment service providers access to information about users' payment accounts, which constitutes personal data. Under PSD2, payment service providers may only access, process and retain personal data necessary for the provision of their payment services with the explicit consent of the user. As explained by the European Data Protection Authorities (European Data Protection Board), this consent should be viewed as contractual consent of the user to conclude a contract with the payment service provider. In accordance with the GDPR, the appropriate legal ground for accessing users' personal data by a payment service provider can be the contract between the two parties.

DNB and the Dutch Data Protection Authority maintain a cooperation protocol where both enforcement authorities set out how they will jointly oversee the personal data processing obligations set out in PSD2 and the GDPR.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

The GDPR applies to the processing of personal data of a company's activities (controller, joint controller or processor) in the EU, irrespective of whether the processing takes place in the EU or not. Furthermore, the GDPR also applies to companies (controller, joint controller or processor) established outside the EU if they: (i) offer goods or services to individuals in the EU; or (ii) monitor the behaviour of individuals in the EU. Thus, an EU fintech company must comply with the GDPR even if it carries out all processing of personal data outside the EU. Similarly, a non-EU fintech company must comply with the GDPR if it provides services to customers in the EU or tracks their behaviour.

The GDPR restricts transfers of personal data outside the EEA unless a country is seen as having an adequate level of personal data protection (an "adequacy decision"). So far, only 14 countries, including the UK, Republic of Korea, Canada, Israel, New Zealand, Switzerland and Japan, are recognised by the European Commission as having adequate protection. In July 2020, the highest court of the EU (Court of Justice of the European Union) invalidated the EU-US Privacy Shield framework that previously facilitated transfers of personal data to the United States. For transfers of personal data to countries outside the EEA that have not been granted an adequacy decision, the data exporter must put appropriate safeguards in place, such as the Standard Contractual Clauses (SCCs) adopted by the European Commission, subject to a prior assessment of whether the law or practice of the third country may impinge on the effectiveness of such clauses. If the law or practice impinges the effectiveness of the clauses, the company must adopt supplementary measures or refrain from transferring personal data. Such prior assessment and, depending on its outcome, supplementary measures are mandatory for all systematic transfers of personal data, including those under Binding Corporate Rules (BCRs). In the absence of appropriate safeguards, personal data can be transferred outside the EEA on the basis of specific derogations, such as the explicit consent of the data subject or the necessity of a data transfer for the conclusion or performance of a contract with a data subject. According to the European Data Protection Board, these derogations can only be used for occasional and not repetitive transfers.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

The GDPR has high penalties for violations of personal data protection rules throughout the EU, and these apply to both controllers and processors. Companies that do not comply with the GDPR are subject to fines of up to EUR 20 million, or 4% of the annual worldwide turnover of an undertaking, per violation, whichever is higher. The European Data Protection Board interprets the concept of "undertaking" broadly – borrowed from EU competition law – to include the whole "economic unit" rather than a legal entity of a data controller or processor. As a result, under certain circumstances, data protection authorities (DPAs) may use the revenue of the whole group to calculate fines under the GDPR. Furthermore, DPAs can also issue temporary or definitive injunctions on data processing and place companies under regular audits.

Companies may also be required to compensate for material and immaterial damages suffered by individuals as a result of a GDPR infringement. Damages claims for data protection violations, filed independently or collectively by individuals, or by not-for-profit organisations on their behalf, present a growing threat to companies with large consumer bases, including those active in the fintech sector. These claims can be filed in parallel or as a follow-on to enforcement by DPAs.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

PSD2 requires that payment service providers have extensive security and reporting requirements in place. First, they must establish a framework with appropriate mitigation measures and control mechanisms, including effective incident management procedures, to manage the operational and security risks relating to the payment services provided. Payment institutions must file with DNB an annual report on the comprehensive assessment of those risks, as well as the adequacy of the mitigating measures and control mechanisms. Second, as a general rule, payment institutions must notify DNB about any major operational or security incident within four hours from the moment the incident was first detected. If the incident has or may have an impact on the financial interest of the users, the payment service provider must, without undue delay, also notify these

users of the incident. In addition, the payment service provider must inform users of all measures they can take to mitigate the adverse effects of the incident.

More generally, the Netherlands has implemented the EU Network and Information Security (NIS) Directive by the Dutch Cybersecurity Act. Both pieces of legislation require operators of essential services and digital service providers to notify serious cybersecurity breaches to the relevant Computer Security Response Team (in the Netherlands, the National Cyber Security Centre) and DNB. This obligation applies to financial institutions that form part of the "financial core infrastructure", including:

(i) credit institutions;
(ii) trading venues (regulated markets, multilateral trading facilities or organised trading facilities);
(iii) central counterparty clearing institutions;
(iv) central security depositories;
(v) providers of settlement services; and
(vi) other financial institutions that play an important role in the transaction chains of these designated services.

Every year, DNB determines which specific organisations in the financial services sector fall under this obligation. Under the Dutch Cybersecurity Act, penalties for violating the cybersecurity breach notification requirement include an administrative fine of up to EUR 5 million.

When it comes to the security of personal data, the GDPR also outlines data security obligations for companies that process personal data, including fintech businesses. These companies must implement "appropriate technical and organisational measures" to ensure a level of security for personal data "appropriate to the risk". The GDPR also requires data controllers to report personal data breaches to DPAs within 72 hours after "becoming aware" of the breach and to data subjects "without undue delay", if their privacy is put at risk.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Please also refer to our explanation at question 3.2. In addition, we note the following.

The two main sources of anti-money laundering law are the Dutch Criminal Code (DCC) and the Wwft.

The DCC defines money laundering quite broadly as: (i) to conceal or hide the true origin, source, location, disposal or relocation of an object, or to conceal or hide who the legal owner of an object is or who possesses the object, e.g. funds; and/or (ii) to acquire an object, have it at one's disposal, transfer, profit from, or use it – both whilst knowing or suspecting (or reasonably should have suspected) that the object originates from a criminal offence, either directly or indirectly. Depending on the degree to which one knew or should have reasonably known, and the frequency in which money was laundered, and whether it was done habitually, the punishment can vary from two to eight years' imprisonment or a fine of up to EUR 90,000, which could, in exceptional circumstance, even be increased to EUR 900,000 (2022), depending on the facts and circumstances of each case.

Dutch AML legislation requires specific businesses and persons to undertake measures to prevent and mitigate risks related to money laundering and terrorism financing. This includes undertaking risk-based customer due diligence before establishing a business relationship, and monitoring that relationship on an ongoing basis. Furthermore, the AML legislation requires relevant businesses and persons to, among other activities, report unusual transactions to the Dutch Financial Intelligence Unit. Infringement of these requirements could result in imprisonment or fines. In addition, the Dutch Minister of Finance may impose an order for incremental penalty payments and administrative fines of up to EUR 5 million per infringement, or EUR 10 million for habitual offenders.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There is no legislation in place in the Netherlands aimed specifically at the fintech sector. The existing regulatory regimes are specific to the activities that a fintech business undertakes. Please see our answers regarding data protection and cybersecurity laws in this chapter, which are relevant to any fintech business.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

The legal framework for the hiring of staff is limited. Several laws prohibit employers from discriminating based on age, sex or religion when hiring employees. There are no set requirements for employment agreements in terms of content, and they can be temporary or permanent. However, certain restrictive provisions (for example, probationary periods and non-competition, unilateral change and penalty clauses) must be agreed on in writing.

Under Dutch dismissal law, there are two ways that an employer can unilaterally terminate an employment agreement:

(i) after obtaining a dismissal permit from the Employee Insurance Agency, giving notice to the employee; or
(ii) requesting that the court dissolve the employment agreement.

The law has nine limited grounds for dismissal, and the relevant ground determines which termination route must be followed.

In order to unilaterally terminate the employment agreement, the employer must demonstrate that there is a reasonable ground for dismissal and that it is not possible to reassign the employee within a reasonable period to a suitable alternative position within the company. An employee is entitled to a statutory transition payment if the employer terminates employment. The transition payment amount depends on the employee's salary and years of service. The transition payment is capped at EUR 86,000 gross, or one annual gross salary if the employee's annual salary exceeds EUR 86,000 gross (2022 figures).

In practice, employment agreements are more often terminated by means of a mutual termination agreement. It is common for employers to pay a severance payment upon termination, which is generally equal to at least the amount of the statutory transition payment.

The dismissal of an employee is prohibited in certain situations, such as during maternity leave, or during the first two years of illness.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Staff are entitled to:

(i) the statutory minimum wage;
(ii) a vacation allowance that is 8% of the employee's annual salary. However, if the employee's salary is over three

times the statutory minimum wage, paying a vacation allowance is no longer mandatory; and

(iii) vacation days four times the amount of days worked per week (20 vacation days per year on the basis of a full-time contract).

During the first two years of illness, employees are entitled to at least 70% of their salary that complies with the statutory minimum wage, and the maximum daily wage (as defined by social insurance law). In practice, many employers pay their employees up to 100% of the employee's salary during the first, and even the second, year of illness. During this period, the employer and employee must work together to reintegrate the employee. After this two-year period, the obligation to pay the salary ends, unless the Employee Insurance Agency finds that the employer did not do enough to reintegrate the employee. In that case, as a penalty, the two-year period in which the employer had to continue to pay an employee's salary can be extended by up to one year.

Mandatory employment benefits can also stem from collective bargaining agreements that apply to a specific industry or to a company or group of companies. It is generally not possible for an employer to deviate from a collective bargaining agreement to the detriment of an employee.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

Employees from EEA countries and Switzerland do not need a work or residence permit to work in the Netherlands. If a company is able to prove that it cannot find any suitable employees within the EEA or Switzerland, it can recruit from other countries. These employees will usually require a work and residence permit.

This does not apply in the case of highly-skilled employees, which is often the type of employee that works for fintech businesses. In order for highly-skilled employees to work in the Netherlands, they can either apply for a "European blue card" or for a Dutch residence permit as a highly-skilled migrant. To obtain a residence permit, the Immigration and Naturalisation Service must recognise the employer as a sponsor. Recognised sponsors can make use of an accelerated application procedure for residence permits. To obtain a European blue card, recognition as a sponsor is not required, but a company can request recognition as a sponsor voluntarily. The highly-skilled migrant has to comply with certain conditions: the employment contract must have a minimum duration of 12 months; it must be for highly qualified work; and the salary must be sufficiently high, among other things.

Please see question 2.2 for the 30% income tax exemption for qualifying expats.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

Innovations and inventions are primarily protected by patents but, depending on the type of innovation or invention, they can also be protected by other intellectual property (IP) rights, such as copyrights (software), database rights and design rights. Know-how and technical information are also protected as trade secrets to the extent the information is kept secret.

Patents

Inventions can be patented for a period of up to 20 years if they are novel, involve an inventive step and are susceptible to industrial application. In contrast to the US, software and business methods are excluded from patentability in Europe. However, an invention devised in a software context can be patentable if it is claimed in the context of the technical system in which it operates (for example, a physical device in which the software is integrated). This framework also applies to AI-based inventions, which are patentable provided that they have a technical character. However, patents for inventions developed by AI have so far been declined by the EPO, as it only recognises persons as inventors.

A Dutch patent may be applied for at the Dutch Patent Office. Dutch patents are not preliminarily reviewed by the Dutch Patent Office and are not subject to opposition proceedings. A Dutch patent can also be obtained as part of a European patent, which consists of a bundle of national patents.

Additionally, the EU patent package – aimed at introducing a European patent with unitary effect in the EU Member States and the Unified Patent Courts (UPCs) – is pending. The European patent with unitary effect is not a bundle of national patents, but can be directly enforced in all participating states, including the Netherlands, through the UPCs. The UPC Agreement requires that 13 participating Member States ratify the agreement for the UPC to exist, including France, Italy and Germany. Only Germany has not yet ratified the Agreement, although it has passed the legislation enabling it to do so. Due to these developments and the start of the provisional application period, the UPC could be constituted as early as September 2022, although it may take longer.

Trade secrets

Information is granted trade secret protection to the extent that it: (i) is secret, meaning it is not generally known or readily accessible; (ii) has commercial value because it is secret; and (iii) has been subject to reasonable measures to keep it secret. This follows from the Dutch Trade Secrets Act that implements the EU Trade Secrets Directive, which in turn is derived from Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs).

Technical data, such as software code and algorithms, can be protected by the Dutch Trade Secrets Act, provided that the abovementioned criteria are met. However, independent creation and reverse engineering do not fall within the scope of trade secret protection. Therefore, if software is to be effectively protected by trade secret law, it is important that the trade secret encompassed within the software is not deducible from its functionalities.

The Dutch Trade Secrets Act provides for protection against misappropriation of trade secrets; that is, the unlawful acquisition, use or disclosure by third parties. The owner of a trade secret has a number of available IP-style remedies, such as injunctions, recalls, damages and evidential seizures. Additionally, actions can be taken against third parties for misappropriation if that party did not know, but should have known, about the misappropriation, or was made aware of the misappropriation after the fact. Furthermore, action can be taken against infringing goods that "significantly benefit" from the misappropriation.

Copyrights, database rights, design rights, trademarks

Except for the protection of the source code of software (which arises by operation of law), copyright plays a limited role in protecting innovations and inventions since technical information regarding functional aspects is exempt from copyright protection. Software code is eligible for copyright protection if

it is original, in the sense that it is its author's own original intellectual creation. This protection also extends to preparatory design work leading to the development of a computer program, provided that no further creative steps are needed in order to create a computer program. The underlying algorithm itself, on the other hand, is not protected by copyright; neither are works resulting from strictly algorithmic processes.

A database is protected by a (unique) database right insofar as the database is the result of a substantial investment in either the obtaining, verification or presentation of its contents ("sweat of the brow protection").

Benelux and Community designs can be relied upon to protect the appearance of a product insofar as the design is novel and has individual character. The branding of innovations and inventions can be protected through trademarks. Trademarks have to be registered. Designs are generally registered rights as well, with the exception of the unregistered Community Design, which has a shorter expiry period than its registered equivalent.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

In principle, the patent applicant is the owner of a Dutch patent. Any other party which claims that it is entitled to the patent can initiate court proceedings.

If an invention was made by an employee, the employee is entitled to the patent unless the nature of the employee's service entails the use of the employee's special knowledge for the purpose of making such inventions. For inventions made during training or by employees of educational or research institutions, the employer and the institution are both generally entitled to the patent. However, this is not mandatory law. Employment agreements generally contain specific clauses to ensure that all inventions and related rights remain or become the property of the employer.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

With regard to IP, various treaties and multi-jurisdictional rights apply in the Netherlands. These include the Paris Convention for the Protection of Industrial Property, TRIPs, the European Patent Convention (EPC) and the Patent Cooperation Treaty (PCT).

Under certain circumstances, Dutch courts can enforce foreign rights (such as patents), but only for the territories in which such rights are valid. For example, a Dutch court can grant an injunction for a German patent, but in that case only with respect to German territory.

As indicated in question 6.1, when the EU patent package becomes effective, it will provide for European patents with unitary effect, which may be directly enforced in the Netherlands.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Licensing is commonly used for monetising IP rights. The licensee generally has the authority to perform the acts that would normally be infringing acts, in exchange for licence fees. The specific details of licensees' rights should, however, be specifically agreed upon in the licensing agreement(s). Specific restrictions relating to patents are compulsory licences, acts with regard to research on the patented matter (the research exception) and prior use. An effective tax rate of 9% may apply for qualifying profits arising from patented or functionally equivalent inventions, subject to a specific regime (please see question 2.2).

Else Loop-Rowel is a senior associate in the Financial Markets Regulation practice group. She specialises in Dutch and EU financial markets regulation, in particular advising banks, insurance companies, investment firms and financial service providers on a wide range of financial regulatory topics such as licence requirements, governance, capital requirements, outsourcings, fit and proper testing, conduct of business rules and discussions with the financial regulatory authorities. Else has also gained significant experience in cross-border M&A transactions involving financial undertakings. Over the years, Else has developed an increased focus on fintech and tech-related questions, including extensive advice on IT outsourcing trajectories and regulatory trajectories with supervisory authorities for fintech companies. She is furthermore part of De Brauw Blackstone Westbroek's fintech focus group, which is part of the Financial Institutions Group.
Her three secondments with large Dutch banks have provided Else with in-depth knowledge on their businesses and insights on the clients' needs *vis-à-vis* their lawyers. She was furthermore elected as one of Elsevier Weekblad's talents under 30 in 2020.

De Brauw Blackstone Westbroek
Claude Debussylaan 80
1082 MD Amsterdam
The Netherlands

Tel: +31 20 577 1541
Email: else.rowel@debrauw.com
URL: www.debrauw.com

Anjali Kaur Doal is a senior associate in the Financial Markets Regulation practice group. She advises large financial institutions, such as banks, investment firms, insurers, pension funds and financial service providers, on a broad range of financial regulatory matters, such as market access and licence requirements, governance, market conduct, business integrity, anti-money laundering (AML), prudential (capital) requirements, and recovery and resolution planning. Anjali is also experienced in financial regulatory aspects of M&A transactions.
Anjali further specialises in innovative technologies (fintech), privacy and data protection-related matters within the financial sector. She is part of De Brauw Blackstone Westbroek's AML practice group and fintech focus group, which is part of the Financial Institutions Group.

De Brauw Blackstone Westbroek
Claude Debussylaan 80
1082 MD Amsterdam
The Netherlands

Tel: +31 20 577 1761
Email: anjali.kaurdoal@debrauw.com
URL: www.debrauw.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group