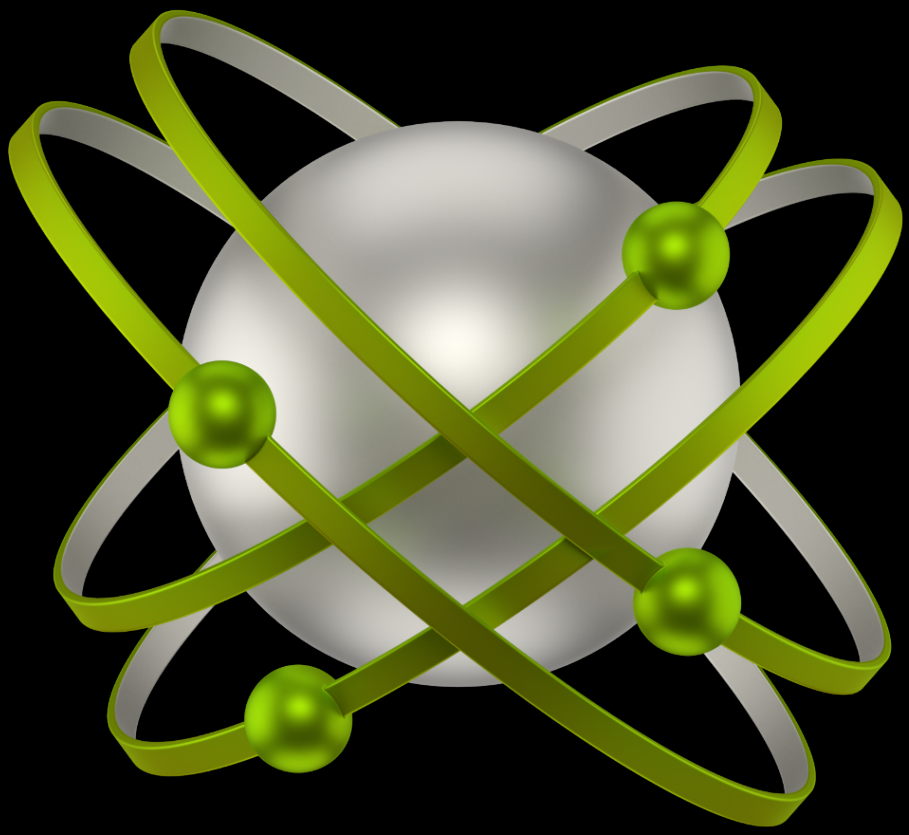
Deloitte.
Legal



Digital banking and banking as a service –

Turkish law compared with European law

March 2022

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

Abstract

Introduction

i. Background of the legislation including the current status of fintech
ii. Comparative law approaches
iii. General approach of the article

Turkey: Regulation on Operation Principles of Digital Banks and Banking as a Service

i. Legal embedding of the regulation
ii. Specifics for digital banking
    01. General principles
    02. Operation restrictions
    03. Additional requirements
    04. Impact on current financial institutions
iii. Specifics of Banking as a Service
    01. Principles and terminology
    02. Specifics

EEA: Framework for digital banking and Banking as a Service

i. Legal embedding
ii. Specifics
    01. CRD
    02. PSD2
    03. DORA
    04. Others (e.g., MiCAR and MiFID)

Comparative evaluation

Implications of the regulation

Summary and outlook

Abstract

Digital transformation in the financial industries is a continuous process affecting products and services provided to end users, internal processes and existing service models. Newly developed and implemented technologies are changing the conventional understanding of the business as well as the interaction with the end-users. Over the past years, the importance of fintech has grown significantly, and this has also affected the legislative background both in European Union ("EU") and Turkey. Recently, Turkish lawmakers have regulated the concepts of digital banking and Banking as a Service ("BaaS") which are seen as the wave of the future. Although the concept of digital banking in particular is often confused with mobile banking and online banking, digital banking is the incorporation of new and developing technologies throughout a financial services entity. In this respect, this article sets out to evaluate the legislation in respect to digital banking and BaaS by making a comparison between EU and Turkish laws, together with the legislative backgrounds.

Introduction

The aim of this section is to analyze the legislative background of fintech in Turkey and the EU by providing information to the readers by way of a general outline of the regulation which came into force in Turkey very recently for digital banking and BaaS.

i.Background of the legislation including the current status of fintech

The main regulation on the banking sector in Turkey is the Banking Law numbered 5411 ("banking law") which entered into force on 1 November 2005[1] and provides the legal framework for banking activities to ensure the reliability and stability of financial markets and to promote the effective functioning of loan markets. The Banking Regulation and Supervision Agency ("BRSA") was established in 2000 as an independent and central supervisory authority to supervise the establishment, management and activities of banks and other financial institutions. The BRSA is vested with the authority and responsibility to protect the rights of depositors while ensuring reliability and stability in the financial markets and promoting the effective functioning of the loan markets. Moreover, the Central Bank of the Republic of Turkey ("central bank"), an independent entity established in 1931, is primarily responsible for the administration of the monetary and exchange rate policies of the Turkish economy.

In Turkey, the promulgation of the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions numbered 6493 dated 20 June 2013 ("law on payment systems") marked an important step in the development of the fintech sector that was created in accordance with the following EU acquis:

01. Directive 98/26/EC
02. irective 2009/110/EC
03. Directive 2007/64/EC ("PSD")

Under an amendment of 22 November 2019 to the law on payment systems, the scope of payment services was expanded to include open banking solutions as well. Additionally, the central bank was authorized to oversee payment institutions and electronic money institutions, instead of the BRSA. Furthermore, as of 1 January 2020 the scope of the central bank's existing supervisory powers was increased under the applicable legislation, thus making the central bank the primary regulator of the payment systems sector and paving the way for open banking.

According to the central bank's official website, there are currently 30 payment entities[2] and 26 e-money entities[3] as of December 2021.

In Turkey, fintech is a growth area, a fact which is also acknowledged by the country's regulators. The most important aspect of consideration for regulators is localization. It is firstly subject to the Regulation on the Information Systems of Banks and Electronic Banking Services published in the Official Gazette dated 15 March 2020 and numbered 31069 ("regulation on the information systems"). In this regard, financial institutions are required to have system and data localization as well as a local presence as prerequisites for obtaining licenses in Turkey. The regulators have published many regulations and laws over the past years which are having a significant impact on the current status of fintech sector in Turkey. Some of the recent, major developments in fintech regulations are:

01. Regulation on the Information Systems, which regulates the management of the information systems used by the banks when performing their activities, as well as the minimum procedures and principles to be established for the performance of electronic banking services and the management of the associated risks along with the information systems controls required for this purpose. The Regulation on the Information Systems also requires banks to keep their primary and secondary systems in Turkey.

02. Regulation on the Generation and Use of TR QR Code in Payment Services published in the Official Gazette dated 21 August 2020 and numbered 31220 ("QR code regulation"). The QR code regulation requires the procedures and principles regarding the payment transactions to be within the scope of payment services in accordance with the law on payment systems rendered through use of a QR code.

03. With respect to crypto-assets, the Presidential Press Release and the Economic Reforms Action Plan published on 12 March 2021 defined crypto-assets and introduced some prohibitions and regulations in this area for the first time in Turkey. It was followed by the Regulation on Non-Use of Crypto Assets in Payments ("non-use of crypto asset regulation") which came into effect on 30 April 2021 and the Regulation Amending the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism, issued by the Financial Crimes Investigation Board regarding crypto-asset service providers, which came into effect on 1 May 2021

04. Regulation on Remote Identification Methods to be Used by Banks and the Establishment of Contract Relationship in Electronic Environment published in the Official Gazette dated 1 April 2021 and numbered 31441 ("regulation on remote identification"), which primarily regulates the procedures and principles for remote identification methods that can be used by the banks.

05. Sharing of Confidential Information published in the Official Gazette dated 4 June 2021 and numbered 31501 ("confidentiality regulation"), which introduces detailed regulations at the point of intersection of the banking law and the Personal Data Protection Law No. 6698 with regard to the confidentiality obligation of persons gaining knowledge of the secrets of banks or their customers in the performance of their duties.

06. Regulation Regarding Payment Services and Electronic Money Issuance and Payment System Service Providers ("regulation on payment services") and the Communiqué Regarding Information Systems of Payment and Electronic Money Institutions and Data Sharing Services of Payment Service Providers ("communiqué") were recently published in the Official Gazette on 1 December 2021 and numbered 31676. The regulation on payment services regulates the procedures and principles regarding the authorization of such payment services and the activities of payment institutions and electronic money institutions, as well as the procedures and principles regarding provision of

    i. Payment services to payment service providers; and
    ii. Electronic money issuance. Additionally, the communiqué introduces regulations regarding the procedures and principles of the management and audit of the information systems that payment institutions and electronic money institutions use when carrying out their activities.

In addition to above mentioned regulations, the Draft Regulation on the Operating Principles of Digital Banks and Banking as a Service was introduced by the Banking Regulation and Supervision Agency ("BRSA") for public opinion on 19 August 2021, and the Regulation on the Operating Principles of Digital Banks and Banking as a Service ("regulation") was published in the Official Gazette on 29 December 2021 and entered into force on 1 January 2022. The regulation aims to set out the principles applying to the long-awaited area of digital banking expected to give rise to a new generation of banking and a service banking model that will enable financial technology companies to offer their financial products and services through the infrastructure of banks.

ii. Comparative law approaches – The Union's stance

Over the years, the growing use of digital platforms in the EU banking and payments sector has been observed. Particularly as a result of the COVID-19 crisis, there has been a significant rise in the digitalization of front- and back-office processes, with financial institutions constantly drawing on the services of third parties and making use of technologies to provide customers with digital access to financial products and services.[4]

However, the European regulatory framework does not follow a specific fintech approach but is rather a fragmented regulatory framework in this regard. In other words, unlike the regulation, which tries to cover digital banking and BaaS under one instrument, the EU encompasses different pieces of legislation covering various topics related to digital banking and BaaS.

Furthermore, the EU approach provides a broad legislative framework to national lawmakers by which the local governments, at their discretion, may introduce their own initiatives. It should be mentioned here that the question of whether or not national lawmakers have such discretion depends on the type of legislative instrument introduced by the respective competent authority of the EU, since a ”regulation” has a binding legal force (in form and content) throughout every member state while a “directive” must be transposed into national laws and each member state has discretion when it comes to how they transpose the directive into national laws.

Even though the laws pertaining to banking in the EU have been harmonized to some extent, the rules governing digital banking have yet to be harmonized. In light of this, the European Banking Authority (“EBA”) in September 2021 published a report on the Use of Digital Platforms in the EU Banking and Payments Sector (“EBA report”). In this report, the EBA identified, among other things, the regulatory perimeter surrounding digital banking as its area of focus and proposes to continuously review the regulatory perimeter, including the treatment of websites at the national level.[5]

This continuous monitoring comes in the light of recent partnership arrangements between banks and fintech companies which are actually classified as “outsourcing arrangements”.[6] From a regulator’s viewpoint it does not matter how such a cooperation was established since it will always be the bank that is “outsourcing” its activities to a non-regulated entity. As a result, regulators will try to identify those sensitive areas which are vital for carrying out fundamental banking or financial services and which otherwise could not be contractually moved to another entity without taking suitable safety measures.[7]

iii. General approach of the article

In the following sections, this article will outline the main principles of the regulation with respect to digital banks and BaaS together with the other laws and regulations referred under the regulation, as well as the European Economic Area (“EEA”) regulatory framework.

Turkey: Regulation on Operation Principles of Digital Banks and Banking as a Service

i.Legal embedding of the regulation

As the name of the regulation indicates, it regulates two main concepts: (i) principles on digital banks, and (ii) principles applicable to the BaaS service model. The regulation is prepared based on the banking law. However, it also makes reference to other laws and regulations which will be applicable to digital banks, service banks and interface providers when conducting or providing services in accordance with the regulation.

More specifically, with respect to digital banking principles the regulation makes clear that, unless otherwise is stated, digital banks are subject to all regulations applicable to credit institutions. With respect to those rules and principles not regulated under the regulation, digital banks will therefore be expected to comply with the other existing primary and secondary laws under banking regulations, including license requirements and permissions. Moreover, the Regulation on Indirect Shareholding and Transactions Subject to Permission of Banks published in the Official Gazette dated 1 November 2006 and numbered 26333 ("regulation on transactions") is referred to in the context of digital banking principles since it is stated that in the regulation the provisions regarding the establishment and operation permit conditions of digital banks will be applicable as additional provisions, without prejudice to the provisions in said regulation. Furthermore, the regulation refers to the Law numbered 6493 on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions published in the Official Gazette dated 27 July 2013 and numbered 28690 ("law numbered 6493") for the determination of the permitted payment institutions and electronic money institutions.

Additionally, chapter three of the regulation refers to some regulations for the requirements and obligations of the parties when conducting BaaS based on the nature of the BaaS service model.

In cases where the agreements are executed electronically by and between the service bank and the customer, service banks must follow the instructions on remote identification as stated under the regulation. For the digital onboarding procedure security criteria, the regulation moreover refers to the Regulation on the Information Systems.

The Regulation on the Procurement of Support Services by Banks published in the Official Gazette dated 05 November 2011 and numbered 28106 ("regulation on support services"), which describes the procedures and principles regarding the purchase of support services by banks by specifying which services are covered under this regulation, together with the banks' obligations and responsibilities when obtaining support services, is also one of the regulations referred under the regulation to define the status of the services obtained by the service bank from interface providers.

For the cases where the service bank transfers customer information to the interface provider, the regulation refers to the confidentiality regulation regarding the confidentiality obligation of persons gaining knowledge of the secrets of banks or their customers in the performance of their duties.

ii. Specifics for digital banking

01. General principles

Digital banks are defined in the regulation as a "credit institution that provides banking services mainly through electronic banking services distribution channels instead of physical branches". According to this definition, digital banks will be allowed to provide services to their customers via internet banking, mobile banking, telephone banking, open banking services, ATMs, and kiosks.

The regulation explicitly provides that digital banks are subject to all regulations applicable to credit institutions unless otherwise stated. That means that with respect to the rules and principles that are not regulated under the regulation digital banks will be expected to comply with the other existing primary and secondary laws under banking regulations.

It is stated that the conditions and requirements for the establishment and operating permit for digital banks shall apply in addition to the requirements laid down by the regulation on transactions, which is the main regulation for the establishment of banks. In other words, the provisions regarding the establishment and operation permit conditions of digital banks in the regulation are applicable as additional provisions, without prejudice to the provisions in said regulation. It is further stated that if the controlling shareholders of the applicants are legal entities that provide technology, electronic commerce or telecommunication services, the BRSA may require the controlling shareholder legal entities or those controlling such legal entities to (i) be resident in Turkey, and (ii) to sign an information exchange agreement with the Risk Center[8] in order to share their risk data regarding the indebtedness and financial power of the persons residing in Turkey.

The minimum capital required for the establishment of digital banks is stated as one billion Turkish liras paid in cash and free from any collusion, and subject to the BRSA's right to increase the amount.

02.Operation restrictions

Some restrictions are outlined in the Regulation for Digital Banks which can be summarized as follows:

a. Customer portfolio

The regulation states that customers of digital banks can only be financial consumers and SMEs. By way of exception, the regulation states that digital banks may extend foreign currency loans to enterprises that are larger than medium-sized enterprises.

b. Organizational restriction

It is provided that digital banks shall open at least one physical office for the purpose of handling customer complaints. However, digital banks are not allowed to organize and open physical branches other than their headquarters and affiliated service units of the headquarters. Such units can be opened only for the purpose of handling customer complaints.

c. Loan restriction

It is stated that the total of unsecured cash loans – excluding expenditures and cash withdrawals made with credit cards and overdraft accounts – that digital banks may make available to a given customer who is a financial consumer cannot exceed four times the average monthly net income of the relevant customer, and that if the customer's average monthly net income cannot be determined the total of unsecured cash loans that can be extended for such customers may not exceed ten thousand Turkish liras.

d. Exception to the operation restrictions

As stated above, the minimum capital required for the establishment of digital banks is one billion Turkish liras, paid in cash and free from any collusion, and subject to the BRSA's right to increase the amount. However, it is stated that if the paid-up capital amount is increased to two billion and five hundred million Turkish liras, digital banks shall be allowed to request an exemption from the mentioned activity restrictions through an application to be made to the BRSA. In such cases, the BRSA's decision on such exemption may provide for banking activities to be carried out by credit institutions fully or partially based on a transition plan.

03. Additional requirements

a. Executive level appointment requirement

The regulation requires the executive holding the highest position with responsibility for the management of information systems to be appointed at least at a hierarchical level equivalent to vice general manager, and to appoint to the board of directors of the digital bank at least one member having more than 10 years of experience in the area of information systems.

b. Activity program and business plan

Digital banks are required to submit the following documentation during the application procedure to the BRSA along with the standard business plan and activity report documents that are required for banks:

- The target audience as determined by the applicant for increasing financial inclusion, such as students, housemakers, youth under the age of 18, SMEs, the needs identified for the groups in this target audience, and the products and services intended to be offered to meet these needs, and its marketing strategy;
- The market size and market gap analysis relating to target audience; and
- The pricing policy for the next five years, the estimated number of customers planned to be acquired, the financial projections and forecast financial statements that predict when the investment will reach the breakeven point and the numerical analyzes showing that

the assumptions forming the basis for these forecasts are reasonable.
- The additional information stated below must be covered in the activity program document:
- Details on general system and network architecture;
- The list of IT systems outsourced to service providers and the risk assessment conducted accordingly;
- Details on customer complaint, request and objection handling procedures; and
- Details on digital onboarding and online identity verification processes.

04. Impact on current financial institutions

The regulation provides that banks currently holding an operating license shall not be entitled to engage in a separate regulatory process to digitize their operations. However, the regulation states that banks that are contemplating to move their operations to digital banking, either partially or completely, must close their existing branches utilizing a plan approved by the BRSA. On the other hand, if banks prefer to carry out their activities only through electronic banking services distribution channels, they must undergo an on-site inspection of the information systems and obtain an affirmative opinion of the relevant BRSA unit on the adequacy of such systems.

Specifics of Banking as a Service

01. Terminology

In the BaaS model, the key parties are identified as “interface provider” and “service bank” and defined as follows:

Interface providers are defined as legal entities that enable their customers to perform banking transactions by accessing the banking services offered by the service bank via the bank's open banking services via the mobile application or internet browser-based interface it has developed. On this basis, an interface provider may be any company that offers services on digital channels regardless of the sector. However, the regulation provides that the service bank can only provide BaaS to interface providers based in Turkey. Based on this limitation, only interface providers established in Turkey are subject to the scope the regulation. Additionally, the regulation states that banks cannot become an interface provider.

Service bank is defined as the bank that offers BaaS services. Based on this definition, service banks may be any bank operating in compliance with the banking law.

With respect to the above-mentioned definitions, BaaS is defined by the regulation as “a banking business model which enables interface providers to act as intermediary for the transactions of the clients through their interfaces and service banks by connecting to the services through open banking services."

02. Principles

The regulation defines the main principles for BaaS as follows:

a. Prohibition of misleading expressions and the requirement of transparency

The regulation explicitly prohibits interface providers from portraying themselves as banks or payment institutions and electronic money institutions in their trade names or in words and expressions that would give the impression that they operate as a bank/payment service provider or that they are collecting deposits, participation funds or funds as a bank/payment service provider in all manner of documents, announcements and advertisements or public statements. This prohibition demonstrates how crucial it is for interface providers to act in a transparent manner when providing their services.

b. Contractual requirements

The regulation sets out the provisions relating to the relationship between the service bank, interface providers and the customers. According to the regulation, a contractual relationship must be established by and between each one of these parties. Additionally, the requirements to be included in the agreements and the obligations of the parties are defined as follows:

- **Agreement between service bank and the customers**

  For the service bank to provide banking services to the customer of the interface provider, an agreement has to be concluded by and between the service bank and the customer. The regulation refers to the Regulation on Remote Identification for cases where the agreement is concluded electronically. Accordingly, remote identification methods to be used by the banks must be followed and the identity of the customer must be determined by the service bank in line with the requirements and obligations specified under Regulation on Remote Identification. Furthermore, the regulation allows this digital onboarding procedure to be completed via the interface provider's application. In that case, however, the service bank and interface provider shall be jointly liable for identity verification and security criteria included in the Regulation on the Information Systems.

- **Agreement between service bank and interface provider**

  01. With respect to outsourcing activities:

  The regulation states that with respect to the services provided by the interface provider to the bank in relation to the services obtained from the bank, as well as its intervention to the agreement to be concluded by and between the bank and its customers or its support enabling the bank to provide its services through its interface, interface providers are hold the position of a support service provider under the regulation on support services.

  Additionally, the regulation states that the service bank, limited to the support services it receives from and the services it provides to the interface provider, can audit the interface provider to ensure the confidentiality and security of clients' confidential information and compliance with the authentication and transaction security criteria in transactions carried out through the service channels of the interface provider. In this respect it is provided that the service bank shall have the right to examine any relevant information, documents, and records of the interface provider.

  The regulation stipulates that an interface provider can provide cloud computing services for the system and data backups only through either (i) a private cloud service model where the hardware and software resources are allocated to the interface provider, or (ii) externally over a community cloud model allowed by the BRSA where the hardware and software resources allocated to organizations subject to the supervision and control of the BRSA are physically shared, but logically assigned separately to each organization.

02. With respect to the customer information sharing:

The regulation states that service bank is required to be compliant with the confidentiality regulation when transferring customer information to the interface provider, which includes the obligation to receive the customer's request or instruction for such action. The confidentiality regulation states that the customer's request or instruction is necessary for disclosure of customer's secret data to third parties resident in Turkey and abroad, and explicit consent does not suffice for such disclosure. The regulation states that the customer's request or instruction may be received in written form or via a permanent data carrier. Provided that the customer is able to cancel or amend its request or instruction at any time and by the same methods used to provide the request or instruction, the customer's request or instruction may be given to cover multiple transactions, and requests or instructions regarding continuous transactions may be given for an indefinite period of time. As a general principle, the customer will be able to query the requests or instructions given through electronic banking channels. For transferring customer information based on a request or instruction, the question of whether or not the principle of proportionality is complied with or not will be determined by inspecting whether the sharing of information respects the customer's request or instruction, provided that the data set requested to be shared by the customer does not contain confidential information relating to other persons.

03. Mandatory provisions to be included in the service agreement concluded by and between the service bank and interface provider:

The regulation stipulates certain mandatory provisions to be included in the service agreement to be executed by and between the service bank and the interface provider. The main provisions to be included in the service agreement are defined as follows:

a. As stated above, the regulation prohibits interface providers from using misleading expressions and requires interface providers to act in a transparent manner in their activities. Accordingly, the service agreement to be executed by and between the service bank and interface provider must state that the interface provider is not a bank or payment service provider holding an operation permit.

b. In the service agreement, it should be clearly stated that the banking services are to be provided by the service bank, along with the services to be offered by the service bank, as well as the responsibilities of the service bank, and the terms of the agreement concluded by and between the service bank and the customer.

c. The obligation of interface provider to make visible on the homepage of its web address: a copy of the type agreement executed by and between the interface provider and the customer, as well as a copy of the type agreement executed by and between the service bank, the logo and name of the service bank from which the service will be received. In the event of the service bank issues a card payment instrument for the interface provider, the bank's name and logo shall be visible on said payment instrument.

– **Agreement between interface provider and customer:**

The regulation states that an agreement by and between the interface provider and customer must be executed and a copy of the type agreement must be published on the website of the interface provider. As stated above, the regulation explicitly prohibits interface providers from portraying themselves as financial institutions in their trade names or words and phrases that would give the impression that they conduct financial activities. Accordingly, interface providers should not use such language or give such impressions in the agreements concluded with the customers.

03. Obligation of service bank to notify the BRSA:

In accordance with the regulation, service banks are expected to publish in their websites a list of the interface providers to which the services will be provided, as well as the scope of services. Additionally, service banks are required to send to the BRSA a copy of the service agreement or its amendments executed by and between the service bank and interface provider within one week from the signing date.

EEA framework for digital banking and Banking as a Service

i. Legal embedding

In the aftermath of the 2008 financial crisis, many harmonized financial market stabilization measures applicable to financial firms throughout the EEA were adopted across Europe. The Commission followed a radical three pillar approach that included the Single Supervisory Mechanism ("SSM"), the Single Resolution Mechanism ("SRM") and – as a third pillar still under discussion – the European Deposit Insurance Scheme ("EDIS"). But specific, comprehensive, and harmonized regulations to address the widespread use of digital technologies and the associated risks in the financial sector have been absent to date. Thus, no legal framework for digital banking and BaaS exists in the EEA today. Even though a few jurisdictions have established a specific regulatory framework for digital banks, most jurisdictions apply the existing banking laws and regulations to banks within their remit, irrespective of the technology they use.

It has to be noted that at the EEA level, BaaS has not been explicitly covered as a topic under any legislation but instead under the purview of "outsourcing arrangement" on which the EBA has provided its guidelines.[9] Furthermore, various regulations and guidelines at the EEA level address and regulate various aspects of digital banking in a fragmented manner, some of which are proposals yet to be adopted. This article briefly discusses these regulations and proposals in the section below.

ii. Specifics

1.CRD

Digital banks essentially undertake the same type of business as any other banks, thus incurring similar risks. Like traditional banks, digital banks may offer a complete range of banking products and services to their clients. Both kinds of banks are authorized to accept deposits and use the deposited money to conduct their banking activities. As a result, they incur similar financial risks, including credit risk, market risk and, to some extent, liquidity risk.[10] Accordingly, digital banks, just like traditional banks, are subject to the requirements stipulated under the Capital Requirements Directive IV ("CRD IV").

The CRD IV applies to credit institutions and covers issues related to supervision, corporate governance, sanctions, market access of credit institutions, as well as large exposures

It is interesting to note that digital banks, like traditional banks, also enjoy the passporting rules. This allows them to provide financial services or establish themselves in other EU

member states under the regulatory supervision of their home country. This concept of the European passport was firmly established in the CRD IV: Articles 17 and 33 stipulate that credit institutions domiciled in another member state of the EU that conduct banking activities[11] in accordance with CRD IV require only a single operating license ("single license") from the competent supervisory authorities of their home member state within the meaning of the Capital Requirements Regulation ("CRR").

On the basis of the single license, they may therefore operate both indirectly by establishing branches in other EU member states and directly by providing cross-border services throughout the entire territory of the EU. By contrast, legally independent subsidiaries still require a separate license in each state.

An analogous regulatory regime also applies under certain conditions to financial institutions domiciled in the EU that are subsidiaries of credit institutions (Article 34 CRD IV).

2. Payment Services Directive ("PSD2")

Over the past few years, open banking has led to the establishment of innovative payment services requiring cooperation and coordination between the servicing payment service providers and third-party providers. However, with more digital payments comes a greater threat to security, and the Second Payment Services Directive, or PSD2, is an attempt to neutralize that threat.

The PSD2 aims to make online card payments more secure in Europe and regulates the relationship between banks and emerging fintech players more actively. The PSD2 has opened the market for payment service providers and requires the banks to cooperate with them. The PSD2 has expanded the EU regulations on electronic payments and now explicitly stipulates cooperation between banks and fintech companies under certain circumstances. One example that illustrates this better is the case in which customers can use an app operated by a payment initiation provider when initiating payment transactions, but in which the transaction is actually executed by the account servicing payment service provider, which is often a bank. This means that services are provided based on more than one regulated payment service provider which are legally and economically separate and required to work together operationally to ensure both the quality and the security of the financial services.

Note that the PSD2 provides for the banks and other traditional payment institutions to give certain emerging service providers access to account information of the customers where such customers have given their consent to this, and this has also been authorized by the relevant supervisory authority.

Further, the PSD2 divides the new service providers into two general categories: (i) payment initiation service providers, which create a software connection between a merchant's website and an online banking platform, and (ii) account information service providers, which enable consumers to review their various bank accounts on a single platform. In other words, the PSD2 requires banks to open their doors to authorized fintech companies irrespective of whether a formal bank-fintech company partnership exists. The European Commission believes that the PSD2 will bring about "more competition, greater choice and better prices for consumers" while guaranteeing improved security and transparency among participants.

3. DORA

After the financial crisis, a uniform set of rules covering large parts of the financial risks associated with financial services was introduced. However, digital operational stability was not fully addressed. Work is now under way to make the European legal space more resilient to attacks on IT systems in order to adapt to advances in technology. So far, various regulations have been adopted, such as the EU Cyber Security Strategy or the Fintech Action Plan. However, the existing EU regulatory framework for information and communications technology ("ICT") risks and operational stability in the financial sector is inconsistent across Europe.

Against this background, the European Commission in September 2020 presented a proposal for a regulation – the Digital Operational Resilience Act ("DORA") – which lays down the plan for having uniform, cross-sector regulations for the management and mitigation of ICT risks at banks and other institutions in the financial sector. DORA aims to further enable and promote the innovation and competitive potential of digital finance while mitigating the potential risks.[12] Moreover, DORA is primarily intended to consolidate and improve the requirements for ICT risks, which were previously addressed in the individual regulations and directives. While these pieces of EU legislation covered the main categories of financial risk (e.g., credit risk, market risk, counterparty credit risk, and liquidity risk), they did not comprehensively address all components of operational resilience when adopted.[13]

According to Article 2, DORA applies among other things, to credit institutions, payment institutions, e-money institutions, investment firms, cryptocurrency providers, etc. In the regulation, all of these institutions and firms are uniformly referred to as "financial entities". The regulation is divided into several chapters. Whereas Chapter I covers general provisions, such as definitions, Chapter II deals with ICT risk management, in particular the requirement for financial entities to have internal governance and control frameworks ensuring effective and prudent management of all ICT risks, as well as comprehensive ICT risk management frameworks. According to Article 6, financial entities shall use and maintain up-to-date ICT

systems, protocols and tools. In addition, the functioning of ICT systems and tools are to be continuously monitored and controlled. Chapter III regulates the handling of ICT-related incidents, in particular the management, classification and reporting of such incidents. Chapter IV further provides that financial entities shall have a robust and comprehensive digital operational resilience testing program as an integral part of the ICT risk management framework. Principles for reliable management of risk from third-party ICT providers are found in Chapter V. Chapter VI details when financial entities can share cyber threat information and intelligence, including indicators of compromise, tactics, techniques and procedures, cybersecurity alerts, and configuration tools.

As DORA will enter into force as part of the Digital Finance Package, it will mark an important step towards the harmonization and digitalization of financial markets in the EU.

Although DORA will contribute to harmonization of the digital finance market, it was not specifically designed to cover the financial market. Technically, large parts of DORA could have been integrated into the governance and risk sections of the special financial services-related directives and regulations. In the coming years, lawmakers and those drafting legislation will have to ensure that future legislative acts avoid inconsistencies between DORA and the specific financial services-related legal framework.

4. Others (e.g., MiCAR and MiFID)

In response to the increasing use of crypto-assets, the European Commission in September 2020 published its proposal for the Markets in Crypto-Assets Regulation ("MiCAR") to regulate crypto-assets uniformly across the EU. The MiCAR is proposed to come into force in 2022 when it will be adopted directly in all member states after a transition period of 18 months.

The MiCAR is proposed to apply to all market participants that issue EU crypto-assets or provide services relating to crypto-assets.[14] Hence, the definition of the term crypto-asset becomes important to determine the applicability. The MiCAR defines a "crypto-asset" as "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology".

Further, the pivotal element of MiCAR is the licensing regime, and accordingly MiCAR establishes regulations on the licensing and supervision of crypto-asset providers and their issuers and is intended to cover the operation, organization, and governance of issuers of asset-referenced tokens and e-money tokens and service providers in the field of crypto-assets. That means that after MiCAR comes into force, entities that have obtained the relevant

authorization from the competent authority and are established in the EU may only provide crypto-asset-related services. These include:
a. Custody and administration of crypto-assets on behalf of third parties;
b. Operation of a trading platform for crypto-assets;
c. Exchange of crypto-assets for fiat currency;
d. Exchange of crypto-assets for other crypto-assets;
e. Execution of orders for crypto-assets on behalf of third parties;
f. Placing of crypto-assets;
g. Reception and transmission of orders on behalf of third parties; and
h.Provision of advice on crypto-assets.

Interestingly, institutions authorized under MiFID II will not be subject to the authorization provisions of MiCAR in respect of crypto-asset-related services. Such institutions may continue to provide services for crypto-assets that they have previously provided under MiFID II without any further authorization obligation. This exemption may prompt upcoming market participants to apply for a license under MiFID II now in order to avoid the future authorization procedure under MiCAR as well as the uncertainties entailed by new legislation.

Comparative evaluation

The regulation has not been able to transpose the EU approach the way it did back in 2020, when the Turkish regulators introduced the “open banking” concept into banking legislation and the legislation on payment systems, payment institutions and electronic money institutions in which they had adapted the advances made by PSD2.

The regulation has made a distinction between digital banking and traditional banking and, as a result, established an entirely new regulatory framework applicable to digital banks in addition to the already existing regulations applicable to credit institutions in the country. This means that digital banks will need to meet additional compliance obligations compared with traditional banks. This is one of the key aspects distinguishing the regulation from EU legislation. In other words, European law currently does not distinguish between digital banking and traditional banking because the European Central Bank holds the view that traditional and digital banks perform the same activities entailing the same risks, the same supervision, and the same regulation. Consequently, the same legislation is applicable to both traditional credit institutions and digital banks in the EU.

Another thing that makes sets digital banks apart from conventional banks is the way in which they deliver their services. Digital banks deliver their services for the most part over the internet and thus rely heavily on digital technologies, connectivity and advanced data capabilities. This results in high technological risks. The EU regulatory framework has identified the increasing risks associated with the technology and have attempted to address them under DORA, as mentioned above. However, such awareness of the technological risk is missing under the regulation.

In our assessment, the regulation has tried to cover, under one umbrella, various aspects, inter alia digital banking, law on credit institutions, BaaS, governance issues, technological risks, etc., without separately working through each area of law in a detailed and comprehensive manner. As a result, the regulation has left some loopholes within the framework which will need to be addressed sooner rather than later. This is another key aspect that distinguishes the regulation from European law. In the EU, digital banking, though not separately regulated, is subject to comprehensive legislation in the form of CRD IV, and the other aspects such as payment services are addressed through an entirely separate piece of legislation. Furthermore, the EBA, through its guidelines, has also tried to cover BaaS under outsourcing arrangements and DORA is a proposal to ensure digital operational stability when it comes to financial services. Such detailed legislative frameworks leave little room for any regulatory loopholes in the EU.

What is also interesting to note is that the regulation is not exhaustive in itself and rather mentions several other pieces of legislations such as the regulation on transactions, law numbered 6493, regulation on support services and confidentiality regulation. Further, these are not mentioned merely for reference purposes but are rather meant to be complied with by the digital banks, which may lead to confusion in the future. Such extensive cross-referencing with far reaching implications is uncommon under European law where legislators usually try to draft the regulatory framework to be extensive, clear and precise, even though they do not always succeed in such attempt.

The regulation showcases the progressive attitude of the Turkish lawmakers as it paves the way for branchless banking and the BaaS model enables financial technology companies to present financial products and services utilizing the infrastructure of conventional banks. On a holistic view, however, there are still some difficult ground to be covered to achieve regulatory convergence with the EU framework, especially considering the advances that MiCAR and DORA will bring with them.

Implications of the regulation

As the concepts of digital banks and BaaS will lead to further fragmentation in the financial service markets, more extensive modification of the business and IT infrastructure will be required. For the last 10 years, the fintech sector has witnessed significant changes throughout the world. Looking at the legislative background and making a comparison between EU and Turkish laws, we see that Turkish lawmakers are mostly using EU legislation as a framework to benefit from the good examples set by the EU. With the implementation of the digital banking and BaaS concepts, traditional banks and financial institutions will be required to compete with the new players from the fintech sector. As a result, new principles will be implemented to create better customer engagement as digitalization and new economic models take hold.

Summary and outlook

As discussed, and commented above, the banking sector system was traditionally focused primarily on transactions and money management. "Today, banking has moved from transactions to experiences that are based on data management - the more insight you glean from the data, the better your ability to deliver engaging client experiences," notes Muralitharan. We think of digital not as a channel, but as the new way of banking, and digital bank not only includes extensive guidance and background on the digital revolution in banking and tracks the innovations and how the mobile internet is changing the dynamics of consumer and corporate relationships with their banks.

The implication is that banks must become digitized, and that is a challenge since becoming a digital bank requires new services focused upon 21st-century technologies and these businesses – both giants and startups – are assertively entering the financial sector, leveraging technology and delivering continuous innovation to frequently upgrade their arsenal and to compete – or collaborate – with banks and other financial institutions in unregulated segments of the financial market or activities that do not require a banking license. Financial institutions must complete a business transformation process by investing in the progressive revamp of their legacy systems to provide the digital services demanded by the emerging generation, while still mitigating reputational and regulatory risk.

In today's world, the banking sector has moved from transactions to create better user experiences by benefiting from the data themselves. Digital revolutions in the banking sector are tracking innovations and changing the dynamics of the user experiences.

One of the biggest challenges for the fintech sector will be focusing on new demands by leveraging technology and delivering continuous innovative solutions to the market. Accordingly, the fintech sector will itself undergo a revolution itself as other players such as startups or other non-financial institutions seek to be a part of this game by becoming competitors or partners of the incumbent banks.

Let's take a look inside the crystal ball: At the very beginning non-financial institutions and incumbent banks were seen as competitors. Many fintech companies tried to gain access to a regulated environment but had to overcome regulatory hurdles that were not part of their ecosystem. Currently, innovative non-financial institutions with a focus on the financial services industry are beginning to partner with innovative incumbent banks offering their regulated ecosystem to innovators. What looks like a good, useful and profitable set-up to be welcomed creates numerous regulatory issues. How can regulators keep a helicopter view on partnerships between incumbent bank and new players that are not directly subject to financial services regulation? A number of regulatory ideas such as sandbox,[15] fintech charters,[16] appointed representative regimes[17] and mentorship[18] have been discussed. Legally speaking, the outsourcing arrangements leading to BaaS or comparable partnerships need to satisfy a specific regulatory regime. Regulators therefore have to address the new partnerships emerging between incumbent banks and non-financial institutions without eliminating their purpose. The Turkish approach may serve as a good starter.

[1]In Turkey, the first law on the banking sector came into force on 1936 and was followed by other laws until 1 November 2005, when the banking law came into effect.

[2]TCMB - Ödeme Kuruluşları

[3]TCMB - Elektronik Para Kuruluşları

[4]EBA September 2021 report on the Use of Digital Platforms in the EU Banking and Payments Sector: https://www.eba.europa.eu/eba-sees-rapid-growth-use-digital-platforms-eu%E2%80%99s-banking-and-payments-sector-and-identifies-steps

[5]EBA September 2021 report on the Use of Digital Platforms in the EU Banking and Payments Sector: https://www.eba.europa.eu/eba-sees-rapid-growth-use-digital-platforms-eu%E2%80%99s-banking-and-payments-sector-and-identifies-steps

[6]Enriques, Luca and Ringe, Wolf-George: "Bank–fintech partnerships, outsourcing arrangements and the case for a mentorship regime", Capital Markets Law Journal, 2020, Vol. 15, No. 4

[7]Enriques, Luca and Ringe, Wolf-George: "Bank–fintech partnerships, outsourcing arrangements and the case for a mentorship regime", Capital Markets Law Journal, 2020, Vol. 15, No. 4

[8]Defined in the banking law as the center established within the organization of the Banks Association of Turkey ("TBB") to collect the risk data of customers of credit institutions and other financial institutions, deemed fit by the BRSA, and to share such data with these institutions, with natural or legal persons themselves or subject to prior consent thereof, private legal persons and third party natural persons.

[9]EBA September 2021 report on the Use of Digital Platforms in the EU Banking and Payments Sector: https://www.eba.europa.eu/eba-sees-rapid-growth-use-digital-platforms-eu%E2%80%99s-banking-and-payments-sector-and-identifies-steps

[10]Ehrentraud, Johannes, Garcia Ocampo, Denise and Quevedo Vega, Camila (2020): "Regulating fintech financing: digital banks and fintech platforms", FSI Insights on policy implementation, no 27, August. 12Annex 1 of CRD IV

[11]Annex 1 of CRD IV

[12]Proposal for a Regulation Of The European Parliament And Of The Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (https://eur lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN), P. 0. 14P 14-15.Therefore, the future DORA Regulation is likely to address the following aspects:

[13]P14-15

[14]Article 2 para. 1

[15]Enriques, Luca and Ringe, Wolf-George: "Bank–fintech partnerships, outsourcing arrangements and the case for a mentorship regime", Capital Markets Law Journal, 2020, Vol. 15, No. 4, page 387 with further reference, inter alia, to Dirk A Zetzsche and others, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation" (2017), Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018534

[16]Enriques, Luca and Ringe, Wolf-George: "Bank–fintech partnerships, outsourcing arrangements and the case for a mentorship regime", Capital Markets Law Journal, 2020, Vol. 15, No. 4, page 389 with further reference to Zaring, David T., Modernizing the Bank Charter (July 31, 2020). William & Mary Law Review, Vol. 61, No. 5, 2020, Available at SSRN: https://ssrn.com/abstract=3664792.

[17]Enriques, Luca and Ringe, Wolf-George: "Bank–fintech partnerships, outsourcing arrangements and the case for a mentorship regime", Capital Markets Law Journal, 2020, Vol. 15, No. 4, page 374 (389) with further reference to the Financial Conduct Authority.

[18]Enriques, Luca and Ringe, Wolf-George: "Bank–fintech partnerships, outsourcing arrangements and the case for a mentorship regime", Capital Markets Law Journal, 2020, Vol. 15, No, page 391. The idea of mentorship regime was first introduced by Enriques, Luca and Ringe, Wolf-George.

Contacts

Dr. Mathias Hanten,
Deloitte Global Banking & Finance Leader – Deloitte Legal

Yaman Polat,
Partner, Deloitte Turkey

Lerzan Nalbantoglu,
Partner, DL Attorneys at Law

Burcu Tumer,
Director, DL Attorneys at Law

Deloitte.
Legal