CATALYST FUND
Powered by BFAGLOBAL

Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Digital Insurance
Mexico

www.bfaglobal.com | @bfaglobal

UPDATED 31 MARCH 2021

Funded by

UKaid
from the British people

Cambridge Centre for Alternative Finance

UNIVERSITY OF CAMBRIDGE Judge Business School

Disclaimer

To the best of our knowledge, the information contained herein is accurate and reliable as of the date of publication.

However, **BFA Global** and the **Cambridge Centre for Alternative Finance** do not assume any liability whatsoever for the accuracy and completeness of the deck, and we provide no warranty, expressed or implied, in respect thereof. The provision of the information contained in this deck does not constitute legal or financial advice or opinions of any kind. No advisory, fiduciary or other relationship is created between us and any person accessing or otherwise using any of the information provided herein. **BFA Global**, the **Cambridge Centre for Alternative Finance**, any of their directors, officers, employees, agents, or contributors will not be liable for any damages, losses or causes of action of any nature arising from any use of any of the said information.

How to use this deck

Relevant regulations

1. Insurance
2. Data protection
3. Consumer protection
4. AML / KYC
5. Cybersecurity
6. Competition
7. Taxation
8. Other relevant regulations

This deck provides **an overview of the various regulations relevant to digital insurance in Mexico.**

Each slide in this deck provides high-level facts about each of the relevant regulations as well as a link to the original source.

The Cambridge Centre for Alternative Finance (CCAF) and BFA Global's Catalyst Fund have developed this deck to help fintech startups working in Mexico and those seeking to enter the Mexican fintech market navigate the regulatory environment.

Cambridge Centre for Alternative Finance
UNIVERSITY OF CAMBRIDGE Judge Business School

01 Insurance

Insurance: **Licensing overview and requirements**

Key regulation: The Law on Insurance and Surety institutions (*Ley de Instituciones de Seguros y de Fianzas* or "LISF"), provides the overarching framework for operators of all types of insurance or bonding institutions, including agents. Secondary provisions are found in the Unique Circular for Insurance and Bonds (*Circular Única de Seguros y Fianzas* or "CUSF")

Main regulator: National Insurance and Bonding Commission (*Comisión Nacional de Seguros y Fianzas* or "CNSF")

Licensing process:

1. Any legal entity seeking to carry on insurance or surety business must be authorized by the CNSF.
2. The licensing fees are:
   a. (i) MXN$52,584.73 (US$2,471.39) for the analysis of the application, (ii) MXN$78,877.10 (US$3,707.09) for the authorization; and (iii) MXN$142,892.40 (US$6,715.69) for starting operations

- Applications must include:
  - Draft articles of association
  - List and information of shareholders.
  - Strategy to implement policies and rules
  - Business plan
  - Proof of having constituted a guarantee deposit in national currency in a credit or government securities institution for its market value for an amount equal to 10% of the minimum paid-up capital with which the company are required to operate.

Minimum capital:

Minimum paid-up capital that institutions must have for each insurance operation is determined by the CNSF.

Agents:

The exercise of the activity of insurance agent or surety agent requires an authorization from the CNSF. Agents include employees, independent contractors, and agent companies.

Sources: Ley de Instituciones de Seguros y de Fianzas, Circular Única de Seguros y Fianza, LEY FEDERAL DE DERECHOS

Insurance: **Microinsurance**

Key regulation:

The Unique Circular for Insurance and Bonds (*Circular Única de Seguros y Fianzas* or "CUSF")

Definition:

Insurance products that provide life, property, casualty, or accident and sickness protection and whose purpose is to promote access to these products for the low-income population through low-cost means of distribution and operation.

Licensing requirements:

The CUSF lists requirements for micro insurers, including:

- Threshold of the insured amount of the microinsurance (ex. in the case of life, accident, and sickness microinsurance, the insured amount shall not exceed 20,000 UDIs).
- Formalities for the specific agreement with the insured
- The content of the policy and some prohibitions, such as the payment of dividends and the establishment of deductibles, co-payments, or any other form of participation of the insured or his/her beneficiaries in the cost of the claim or service

Licensing fees:

The licensing fees for micro insurance agents are MXN$3,711 (US$174) for natural persons and MXN$11,798 (US$555) for legal entities.

Sources: Circular Única de Seguros y Fianza, LEY FEDERAL DE DERECHOS

Insurance: **Adjusters**

- Adjusters are persons who investigate insurance claims on behalf of an insurer to determine the extent of the insurer's liability. They may be a natural person or a legal entity.
- To be appointed as an insurance adjuster, the insurance institution is required to verify that the natural person carrying out such activity is of legal age, is of good repute, and has accreditable knowledge of the corresponding subject matter, enabling him/her to carry out the activity. Insurance institutions may only appoint persons registered with the CNSF as adjusters for insurance contracts related to adhesion contracts.
- Insurance companies are required to create manuals detailing the guidelines, policies, and procedures adjusters must observe and publish the manuals on their website.
- Insurance institutions are responsible for the performance of the insurance adjusters they appoint within the scope of their activity.

Source: Ley de Instituciones de Seguros y de Fianzas

02 Data protection

Data protection: **National provisions**

Key Laws:

Federal Law on Protection of Personal Data Held by Individuals (*Ley Federal de Protección de Datos Personales en Posesión de Particulares* or "LFPDPPP") for private sector

Main definitions:

- Processing data is defined as: "the collection, use, disclosure or storage of personal data, by whatever means. Use includes any action of access, handling, use, exploitation, transfer, or disposal of personal data."
- Personal Data is defined as: "any information concerning an identified or identifiable natural person."
- Sensitive Personal Data is defined as "those personal data that affect the most intimate sphere of their owner or whose improper use may give rise to discrimination or entail a serious risk for the owner. In particular, data that may reveal aspects such as racial or ethnic origin, present and future state of health, genetic information, religious, philosophical and moral beliefs, trade union membership, political opinions, or sexual preference are considered sensitive."

Main provisions:

- Personal data may only be processed if the principles of lawfulness, consent, information, quality, purpose, loyalty, proportionality, and responsibility are met.*
- Any controller who processes personal data is required to establish and maintain administrative, technical, and physical security measures to protect personal data against damage, loss, alteration, destruction, or unauthorized use, access, or processing

*The principles of lawfulness, consent, information, quality, purpose, loyalty, proportionality and responsibility are defined in either the LFPDPPP or its secondary provisions.

Source: Ley Federal de Protección de Datos Personales en Posesión de Particulares

Data protection: **Sectoral provisions**

There are also data protection provisions in financial service sector-specific regulation

Crowdfunding:

- **The General Provisions Applicable to Financial Technology Institutions** require that crowdfunding applicants provide evidence that their personal data controllers have implemented personal data protection and data privacy policies.

Novel Models:

- **General Provisions relating to Companies Authorised to Operate Novel Models** establish that applicants for an authorization to operate Novel Models are required to provide Operational Contingency and Information Security Incident Management Policies, which are required to contain procedures for reporting such situations to the CNBV.

Marketing/Advertising:

- **General Provisions of the CONDUSEF on Transparency and Sound Practices applicable to Financial Technology Institutions** require fintech institutions to obtain consent in order to use personal data for marketing, advertising, or any other purpose; Fintech institutions must obtain the prior authorization of the user independent of the contract of adhesion of services or products.

Sources: DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA, DISPOSICIONES DE CARÁCTER GENERAL RELATIVAS A LAS SOCIEDADES AUTORIZADAS PARA OPERAR MODELOS NOVEDOSOS A QUE HACE REFERENCIA LA LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA, DISPOSICIONES de carácter general de la CONDUSEF en materia de transparencia y sanas prácticas aplicables a las instituciones de tecnología financiera.

Data sharing: **Open finance**

- Open Finance is set out in Article 76 of the Fintech Law.
- Financial institutions, money transmitters, credit information companies, clearing houses, fintech institutions, and companies authorized to operate with Novel Models are required to establish standardized computer application programming interfaces ("**APIs**") that enable connectivity and access to other APIs developed or managed by the same set of authorized companies and third parties specializing in IT to share the following data and information:
    - **Open financial data**: data concerning products and services offered to the general public, including the location of offices and branches, ATMs, or other access points to their products and services. The specific secondary provisions for Open Financial Data APIs are accessible here.
    - **Aggregated data**: data related to any type of statistical information concerning operations, without a level of disaggregation that an individual's personal data or transactions can be identified.
    - **Transactional data**: data related to a customer's use of a product or service, including deposit accounts and credits.
- For a participant to access information through APIs, prior authorization is required from the Supervisory Commissions (*Comisiones Supervisoras*) or from Banxico for credit information companies and clearing houses.
- The Supervisory Commissions or, where appropriate, Banxico, are required to approve the fees charged by the entities for the exchange of data and information. These fees must be equitable and transparent.
- In Mexico, the approach towards "Open Finance" is generally broader in scope in comparison to other jurisdictions. The Open Finance framework is not only available to banks, but also to all other financial institutions and third parties specialized in IT, including 'BigTechs'.

Source: Ley para Regular las Instituciones de Tecnología Financiera

03 Consumer protection

Consumer protection: **National provisions**

Key Law:
Consumer Protection Federal Law (1992) intends to promote and protect the rights of the consumer and a culture of responsible and intelligent consumption and to ensure fairness, certainty, and legal security in relations between suppliers and consumers.

Key Regulator:
The Federal Consumer Protection Agency (*Procuraduría Federal de Protección al Consumidor* or "PROFECO") promotes a culture of responsible and intelligent consumption, so consumers are in a position to make good and sufficiently informed decisions about the consumption of goods and services and the rights to which they are entitled.

PROFECO
PROCURADURÍA FEDERAL DEL CONSUMIDOR

Source: LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR

Consumer protection: **Sectoral provisions**

Key Law:
The Law for the Protection and Defence of the User of Financial Services (*Ley de Protección y Defensa al Usuario de Servicios Financieros)*

Key Authority:
The National Commission for the Protection and Defence of Financial Services Users (*Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros* or "CONDUSEF") is responsible for ensuring fairness in relations between users and financial institutions.

Focus on fintech:
CONDUSEF's general provisions on transparency and sound practices apply to fintech institutions (*Disposiciones de carácter general de la CONDUSEF en materia de transparencia y sanas prácticas aplicables a las instituciones de tecnología financiera)*

Other provisions
There are specific provisions regarding the creation of Taxpayers' Ombudsman's Office (Procuraduría de la Defensa del Contribuyente or "PRODECON") and labor dispositions regarding the creation of Federal Labour Ombudsman's Office (Procuraduría Federal de la Defensa del Trabajo or "PROFEDET").

Sources: Ley de Protección y Defensa al Usuario de Servicios Financieros, Disposiciones de carácter general de la CONDUSEF en materia de transparencia y sanas prácticas aplicables a las instituciones de tecnología financiera, Website PRODECON, Website PROFEDET

04 Anti-money laundering (AML)/know your customer (KYC)

AML/KYC: **Key laws & main provisions**

Key Laws:
Federal Law for the Prevention and Identification of Operations with Resources of Illicit Proceeds (LFPIORPI)

There are also specific AML/FT regulations for each type of financial institution

Main provisions for non-financial institutions:
LFPIORPI identifies some "vulnerable activities"* of non-financial institutions within the Mexican markets that are subject to special regulation, which include:

- The issuance or marketing, on a regular and/or professional basis, of service cards, credit cards, prepaid cards, and other instruments for the storage of monetary value that are not issued or marketed by financial institutions. This activity reports to the SHCP when a specific threshold (approximately US$5,758.00 in monthly expenditure) is passed.
- The regular or professional offering of mutual or guarantee loan operations or granting of loans or credits by subjects other than financial institutions. This activity reports to the SHCP when a specific threshold (approximately US$7,190.00) is passed.
- The regular and professional offering of exchange of virtual assets by subjects other than financial institutions, which are carried out through electronic, digital or similar platforms. This activity reports to the SHCP when a threshold (approximately US$2,800.00) is passed

Main provisions for financial institutions:
The specific AML/FT regulations require banks and other financial institutions to adopt international policies – specifically Financial Action Task Force ("FATF") recommendations and guidelines – that indicate their commitment to AML/CFT requirements provided by law and secondary regulations. They also must set up internal control measures such as:

- the appointment of a Compliance Officer or a Communication and Control Committee,
- the generation and application of a Control Manual for AML/CFT purposes, and
- the establishment of a risk-based approach, and analysis, generation of a model, and methodologies applying this approach, among others.

Geolocation requirement:
As of March 21, 2021, CNBV requires financial institutions to obtain and keep the real-time geolocation of the devices their customers use to carry out operations or services. This requirement will be implemented by sector in a staggered manner.

*All the thresholds provided above for vulnerable activities are measured by the minimum wage in force in Mexico City except the final "vulnerable activity" – virtual assets – which is measured in Measurement and Update Units ("UMAs"), whose value is published by the National Institute of Statistics and Geography ("INEGI") every year

Sources: Federal Law for the Prevention and Identification of Operations with Resources of Illicit Proceeds, Federal Law for the Prevention and Identification of Operations with Resources of Illicit Proceeds, Inicia la implementación de la geolocalización de dispositivos para operaciones financieras, specific regulations AML/FT provisions for each type of financial institution

AML/KYC: **Customer due diligence requirements**

- Customer Due Diligence (CDD) requirements for financial institutions depend on the type of financial institution.
- **At a minimum the mandatory KYC requirements for an individual are:**
  - **a.** The following identification data, obtained from a valid document:
    - **i.** Paternal surname, maternal surname and first name or names without abbreviations
    - **ii.** Gender
    - **iii.** Date of birth
    - **iv.** State of birth
    - **v.** Country of birth
    - **vi.** Nationality
    - **vii.** Voter ID number, if applicable
  - **b.** Proof of residence
  - **c.** Occupation, profession, activity, or line of business in which the client is engaged
  - **d.** Unique Population Registry Code
  - **e.** Advanced Electronic Signature Serial Number, if the client has one
  - **f.** Telephone number
  - **g.** E-mail address
  - **h.** If applicable, account number and Standardized Banking Code (CLABE) in the Financial Entity or Foreign Financial Entity. Financial Institution or Foreign Financial Institution authorized to receive deposits.
  - **i.** Establish in the ITF's Terms and Conditions that the natural person is acting on his/her own behalf and account.

Sources: Prudential Guidelines For Institutions Licensed Under the Banking Act, GSMA Proportional risk-based AML/CFT regimes for mobile money; For Banks: General Provisions referred to in Article 115 of the Credit Institutions Law (AML provisions for Banks); For Fintechs: General Provisions referred to in Article 58 of the Law to Regulate Financial Technology Institutions (AML provisions for Fintech institutions).

AML/KYC: **Customer due diligence requirements (cont.)**

Additional due diligence measures that may be used to verify the identity of the customer include:

Copies of the following documents can be used for verification:

- Personal identification
- Proof of Unique Population Registry Code
- Proof of address
- Declaration of the natural person that he/she is acting in his/her own name and on his/her own account or on behalf of a third party, as the case may be.

What is the situation of remote (i.e. non face-to-face) CDD by mobile phone?

- For banks and fintech institutions conducting digital onboarding, institutions shall require and obtain from their clients the geolocation of the mobile device from which the client opens the account, the consent for engaging in the digital onboarding, and the voter identification number (for banks).
- Regarding accounts classified as level 2 that are contracted remotely, banks are required to integrate the identification files of their clients with other data, including the full name without abbreviations, gender, state of birth, date of birth, and their domicile.

Sources: For Banks: General Provisions referred to in Article 115 of the Credit Institutions Law (AML provisions for Banks); For Fintechs: General Provisions referred to in Article 58 of the Law to Regulate Financial Technology Institutions (AML provisions for Fintech institutions).

AML/KYC: **Simplified customer due diligence**

Fintech Institutions:

- The accounts or contracts offered by fintech institutions to their clients may be considered low risk and, therefore, may only require a simplified identification regime, provided the following:
  - In the case of accounts or contracts classified as level 1 and entered into with natural person clients with transactions limited to 750 Investment Units (UDIs) (MXN$5,161/US$258) over a calendar month, the fintech institution shall only be obliged to collect the paternal surname, maternal surname and name or names without abbreviations, date of birth, gender, federal entity, occupation, profession, activity or line of business, and e-mail address.
  - Level 1 accounts or contracts shall be subject to a maximum balance equivalent of 1,000 UDIs (MXN$6,899 or USD$345).
  - In the case of accounts or contracts classified as level 2 and entered into with natural person clients with transactions limited to 3,000 UDIs (MXN$20,646/US$1032) over a calendar month, the fintech institution shall only be obliged to collect, in addition to the data indicated above, the client's address and the digital version of the document from which the client's identification data originate.

Banks:

- Deposit accounts in national currency offered by the entities are considered low risk and, therefore, may have simplified identification requirements if they are subject to the following:
  - In the case of accounts classified as level 1 that are opened by natural person clients, whose operation is limited to credits equal to 750 UDIs (MXN$5,161/US$258) per client, per calendar month, the entities may integrate the respective identification files of their clients, only with the data of their paternal surname, maternal surname, name or names without abbreviations, and date of birth.
  - In the case of accounts classified as level 2 that are opened by clients who are natural persons, whose operation is limited to credits equal to 3,000 UDIs (MXN$20,646/US$1032) per client, per calendar month, the entities may integrate the respective identification files of their clients only with data relating to the full name, without abbreviations, date of birth, and address. In this case, the data relating to the name and date of birth of the customer must be obtained from an official identification.

Sources: For Banks: General Provisions referred to in Article 115 of the Credit Institutions Law (AML provisions for Banks); For Fintechs: General Provisions referred to in Article 58 of the Law to Regulate Financial Technology Institutions (AML provisions for Fintech institutions).

05 Cybersecurity

Cybersecurity: **Relevant legislation**

Cambridge Centre for Alternative Finance
UNIVERSITY OF CAMBRIDGE Judge Business School

National legislation:

- There is no national regulatory framework for cybersecurity.
- Notwithstanding, there is an advanced initiative for instituting a General Cybersecurity Law.
  - The initiative proposes creating a permanent cybersecurity commission within the National Public Security Council, which will be responsible, together with the Executive Secretariat of the National Public Security System, for monitoring compliance with the actions of the National Cybersecurity Center, a new entity also created by this new Law, which has the mandate to monitor, prevent and manage cybersecurity risks, dangers and threats arising within and outside the national territory.
  - The National Cybersecurity Center will be responsible for developing a national cybersecurity strategy in collaboration with the telecommunications regulator, the Federal Telecommunication Institute (*Instituto Federal de Telecomunicaciones* or "IFT").
  - Article 23 of the initiative proposes that users are required to provide real identity information when signing agreements or confirming receipt of services from network providers, companies that manage access to the fixed or mobile telephone network, or firms that provide information, publishing, or instant messaging services, such as Facebook, Twitter or WhatsApp. The initiative warns: "*where users do not provide real identity information, network operators will not provide the services*."

Sectoral Legislation:

- There are sectoral provisions, such as the General Provisions Applicable to Electronic Payment Fund Institutions related to Security of Information, that lay out technical specifications for the technological infrastructure of fintech institutions, Chief Information Security Officer (CISO) faculties and responsibilities, data localization specifications, and technical requirements for two-factor authentication (2FA).

Sources: Draft General Cybersecurity Law, DISPOSICIONES APLICABLES A LAS INSTITUCIONES DE FONDOS DE PAGO ELECTRÓNICO A QUE SE REFIEREN LOS ARTÍCULOS 48, SEGUNDO PÁRRAFO; 54, PRIMER PÁRRAFO, Y 56, PRIMER Y SEGUNDO PÁRRAFOS DE LA LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA

Cybersecurity: **Data Localization Specifications**

In the event of a partial or temporary interruption in the cloud computing service with a foreign provider, IFPEs must provide within their Business Continuity Plan a mechanism to ensure the continuity of services for their clients and guarantee they will maintain the necessary computing and processing capacity within two hours of any outage. The requirements apply to IFPEs that meet any of these descriptions:

- Carry out more than 3.5 million transfer transactions.
- Send or receive transfers of a total amount greater than the equivalent in local currency of 6 billion UDIs (MXN$41,291,334,000.00/ US$2,064,566,700.00).
- At any time, have had more than one million accounts that, at any time during a twelve calendar month period, have registered a positive balance or sent at least one transfer or have had a total balance in the accounts exceeding 400 million UDIs (MXN$2,752,755,600.00/US$137,637,780.00).

The mechanisms to be implemented are:

- Engaging an additional cloud computing provider that is incorporated in and subject to a different jurisdiction than the original cloud computing service provider and that is under the control of a person other than the original provider.
- A mechanism that allows the IFPE to have its own infrastructure that enables it to carry out, in a territory other than that of the foreign jurisdiction in which the risk may occur, the processes referred to without this implying simultaneous operation with the cloud computing used in its normal operation.
- Any mechanism other than those referred to above that, at the request of the IFPE, is authorized by the Mexican Central Bank and the CNBV, provided that the IFPE demonstrates that such mechanism can ensure continuity in the performance of the acts necessary to issue, transmit, redeem or manage electronic payment funds, in the event of interruption for the causes indicated therein.

Sources: General Provisions Applicable to The Electronic Payment Fund Institutions Referred to in Articles 48, Second Paragraph, 54, First Paragraph, and 56, First and Second Paragraphs of the Law to Regulate Financial Technology Institutions (Security Provisions)

06 Competition

Competition: **Relevant legislation & competition issues**

Relevant authority & legislation:

- The Federal Economic Competition Commission (*Comisión Federal de Competencia Económica* or "COFECE")* seeks to ensure free and economic competition and prevent, investigate, and combat monopolies and other restrictions on the efficient operation of markets in Mexico.
- The Federal Competition Law (*Ley Federal de Competencia Económica* or "LFCE") is the primary antitrust legislation. LFCE covers restrictive agreements, abuse of dominant position, monopoly, and price regulation.
- LFCE requires that:

1) Marketing and testimonials are not misleading or deceptive,
2) Goods and services are not displayed without the price, and
3) Products/services are not bundled together, unless it can be demonstrated that the convenience of bundling to the consumer outweighs the limits bundles place on the consumer's right to choose, among other requirements.

- The abuse of a dominant position in a market is prohibited. The consequences of abuse includes a notice to the firm to cease abusive practices. Abuse is also considered an offence and the penalties are up to 10% of the firm's turnover in the preceding business year or a higher percentage as determined by a court.

*In December 2020 COFECE approved, without conditions, the majority acquisition of Cornershop Mexico by Uber. Prior to this acquisition, there was litigation to establish which authority, IFT (Ministry of Telecommunications) or COFECE, was in charge of analyzing the digital platform market. It was held that COFECE was competent, so COFECE is the responsible competition authority for digital platforms market.

Sources: Ley Federal de Competencia Económica, Cornershop Mexico/ Uber Acquisition, Resolution in favor of COFECE

07 Taxation

Taxation: **Financial services**

Relevant taxes:

- Mexican tax laws may apply to fintech activities. These regulations include the Income Tax Law (LISR), the Federal Tax Code (CFF), the Value Added Tax Law (LIVA), and the General Provisions called "Miscellaneous Tax Resolution" (*Resolución Miscelánea Fiscal* or "RMF").
- Individuals and legal entities that carry out the following activities on national territory must pay the value added tax (VAT) established in LIVA:
  - Disposal of assets.
  - Provide independent services.
  - Grant the temporary use or enjoyment of goods.
  - Import goods or services.

Application to Fintech:

- In the RMF, there are certain reforms to the LISR and LIVA that directly affect services offered via online platforms. As of June 1st, 2020, foreign companies that provide digital services to users in Mexico through digital applications are required to charge VAT for such services.
- Similarly, if national or foreign technological platforms provide intermediation services in addition to providing digital services, they will be obliged to withhold both Income Tax (*impuesto sobre la renta* or "ISR") and VAT from individuals who sell goods or provide services, including hosting services and to report these withholdings to the Tax Administration System (*Sistema de Administración Tributaria* or "SAT").

Sources: LEY DEL IMPUESTO SOBRE LA RENTA, CÓDIGO FISCAL DE LA FEDERACIÓN, LEY DEL IMPUESTO AL VALOR AGREGADO, Resolución Miscelánea Fiscal - RMF

08 Other relevant regulation

Other relevant **company regulations**

- **Incorporation of companies** - The main regulation is the General Law on Commercial Companies.
- **Employment of foreign employees** - If a fintech firm wishes to employ foreign individuals, they are required to comply with the provisions of the Migration Law.
- **Intellectual Property** - The Federal Law for the Protection of Industrial Property deals with trademarks, patents, industrial designs, and their specific protection schemes.
- **Copyright** - The Copyright Law creates a process to obtain copyright protection of computer programs.
- **Foreign Investment Law -** This law sets out rules on foreign exchange, including transactions and investment of foreign currencies in Mexican businesses.
- **Labor Law** - The relevant regulation is the Federal Labor Law. There are also new specific regulations for working from home due to the pandemic:
  - Decree reforming Federal Labour Law on Remote Working
  - Psychosocial risk factors at work - Identification, analysis and prevention

Sources: LEY GENERAL DE SOCIEDADES MERCANTILES, LEY DE MIGRACIÓN, LEY FEDERAL DE PROTECCIÓN A LA PROPIEDAD INDUSTRIAL, LEY FEDERAL DEL DERECHO DE AUTOR, LEY DE INVERSIÓN EXTRANJERA, LEY FEDERAL DEL TRABAJO, Pandemic Regulations

Other regulations: **Virtual and crypto assets**

- **Regulatory Approach.** Banxico issued Circular 4/2019 which permits banks and fintech institutions to enter into virtual asset internal transactions - also known as *back-office transactions* - only with prior authorization granted by Banxico. Banks and fintech institutions are prohibited from conducting direct virtual asset transactions with clients or offer virtual asset custody, control, or transmission services to such clients.
- **Definition under the Fintech Law.** "A virtual asset is an electronically recorded representation of value used by the public as a means of payment for all types of legal acts, the transfer of which may only be carried out by electronic means. Under no circumstances shall a virtual asset be understood to be legal tender in national territory, foreign currency, or any other asset denominated in legal tender or foreign currency."
- **Limitation.** Fintech institutions are only permitted to operate with virtual assets that are approved by Banxico. In addition, fintech institutions and banks cannot provide virtual asset exchange, transmission, or custody services to their clients.
- **Need to provide a disclaimer.** Fintech institutions that manage virtual assets must disclose to their clients the risks of such transactions. Disclaimers must be posted on the fintech institution's website:
  - The virtual asset is not legal tender and is not backed by the Federal Government or Banxico.
  - The impossibility of reversing transactions once executed, if applicable.
  - The volatility of the value of the virtual asset.
  - The technological, cyber, and fraud risks inherent to virtual assets.

Sources: Circular 4/2019, Ley para Regular las Instituciones de Tecnología Financiera

For more information and further guidance on engaging with regulators see [Fintech Regulation in Mexico]

www.bfaglobal.com
info@bfaglobal.com
@bfaglobal