Alert | Financial Regulatory & Compliance

June 2020

New Open Banking Regulation in Mexico

Leer en Español.

New regulations have been recently issued pursuant to Mexico's Law to Regulate Financial Technology Institutions, published March 10, 2018 (the "Fintech Law" or the "Law"). These new regulations apply to a significant group of financial entities and require the establishment of application programming interfaces ("APIs") to enable connectivity, access, and sharing of certain data.

All financial entities explicitly mentioned by the Fintech Law[1] are subject to data sharing requirements, as are money transmitters, credit reporting agencies, payment switches regulated by the Law for the Transparency and Ordering of Financial Services, and financial technology institutions (i.e., crowdfunding and e-money companies (wallets)), as well as companies operating under a *sandbox* approval, as provided by the Law (the "Regulated Entities"). These changes reflect a general trend in the regulation of banks and e-money institutions to ensure compatibility and open standards between the payment institutions and other technology providers, as can for example also be seen in Artt. 35 and 36 of the European Union

---

[1] Bank-holding and subholding companies, banks, broker-dealers, exchanges, mutual funds and their distributors, credit unions, auxiliary credit institutions, exchange houses, non-bank lenders (SOFOMs), popular and community financial entities, agrofinancing integrators, cooperatives, securities deposit institutions and clearinghouses, rating agencies, insurance and bonding companies, pension funds and other institutions or public trusts conducting activities subject to the supervision of the CNBV, the CNSF or the CONSAR.

Second Payment Services Directive (commonly referred to as PSD2). As can be seen, the regulatory framework in many territories such as the European Union and now also Mexico is adapted to encourage new fintech business models.

The types of data to be shared under the Law are as follows:

- **Open data:** Information generated by the Regulated Entities that does not contain confidential information, e.g., general information on the products or services offered and the location of their offices, branches, ATMs and other points of access to their products and services;

- **Aggregated**: Statistical information on transactions conducted by or through Regulated Entities which is presented in a way that prevents personally identifiable information (PII) or individual transaction records to be exchanged; and

- **Transactional**: Data related to the use by clients of the Regulated Entities of a specific product or service, including deposit accounts, loans and other means of withdrawal, which data constitute PII and therefore may only be shared with clients' prior consent (which shall specify the purpose of sharing).

APIs are the pillar of the *open banking* principle adopted in multiple jurisdictions to foster competition in financial markets. Under the Law, the Mexican Central Bank ("BANXICO") shall issue the secondary regulation for the exchange of data by credit reporting agencies and payment switches, and the commission in charge of regulating and supervising a financial industry[2] (each, a "Supervisory Commission") shall issue the regulation for the financial entities in that industry. Accordingly, the following regulations have been recently issued:

  – Regulation 2/2020, which contains the *General Provisions referred to in Article 76 of the Law to Regulate Financial Technology Institutions, applicable to Credit Reporting Agencies and Switches related to Application Programming Interfaces* ("Regulation 2/2020") issued by BANXICO on March 10, 2020; and

  – *The General Provisions relating to Application Programming Interfaces referred to by the Law to Regulate Financial Technology Institutions* issued by the CNBV and effective as of June, 5 2020 (the "CNBV Regulations" and, together with Regulation 2/2020, the "Regulations"), which apply to the rest of the Regulated Entities, fintech companies and companies operating under a *sandbox* approval, and money transmitters, as well as third parties specializing in information technology (in the latter case, acting only as "Data Petitioners").

Pursuant to the Fintech Law, Regulated Entities must obtain approval from the competent Supervising Commission or from BANXICO, in the case of credit reporting agencies and switches, to gain access to other Regulated Entities' APIs. This implies the need for consideration for the exchange of information registered and the adoption of adequate processes for the exchange of information. The objective of the Regulations is to define the legal framework for those approvals and processes.

---

[2] The National Banking and Securities Commission ("CNBV"), the National Retirement Savings System Commission ("CONSAR"), the National Insurance and Bonding Commission ("CNSF") and the National Financial Consumer Protection Bureau ("CONDUSEF"), each in its respective jurisdiction.

Regulation 2/2020

This regulation sets forth the standards for the interoperability of APIs used by the Financial Entities to which it applies (i.e., credit reporting agencies and switches), as well as for determining the technical information for such interoperability, but deals only with the exchange of open and aggregated data. The following are the main topics that it regulates:

(a) Requirements for the approval of APIs for the exchange of open, aggregate, and transactional data (including the need to submit a business plan and form interconnection agreements, as well as to have a BANXICO-approved digital certificate for the reporting of information to such regulator);

(b) Requirements for other Regulated Entities to gain access to the data of the entities subject to it through their respective APIs;

(c) The minimum requirements for interconnection agreements;

(d) The obligation to register consideration to be charged to third parties in exchange for data (which consideration shall be equitable and transparent), as well as BANXICO's authority to make observations on new or increased consideration schemes (and even to veto their application when its observations have not been satisfied); and

(e) BANXICO's supervisory authorities, which include the power to suspend the exchange of information, and the minimum requirements of compliance remediation (*regularización*) programs for entities to implement in response to such a suspension.
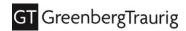
In general, entities subject to this regulation have 360 days as from its entry into force (which will in turn be 360 days after its publication) to obtain approval from BANXICO for the establishment of their respective APIs.

As an exception to the above, entities subject to this regulation who wish to obtain approval for the exchange of transactional data shall (i) first obtain approval for the exchange of aggregated and open data, if applicable; and (ii) within 360 days after the publication of the regulation (i.e., before it comes into force), submit proposals as to the type of data that should be considered transactional, as well as on the mechanisms through which such entities would plan to authenticate, identify, and obtain express consent from the respective clients, if applicable. Based on this, BANXICO will subsequently issue a new set of general provisions governing the sharing of transactional data by the entities subject to Regulation 2/2020 through their respective APIs and the obtaining of the corresponding client consents.

CNBV Regulations

These provisions only regulate the sharing of open data, which by definition does not contain confidential information and the free sharing of which does not constitute a risk for those who generate it. Consequently, the CNBV Regulations are aimed at establishing simpler ways of complying with the Fintech Law and avoiding unnecessary formalities and additional costs in obtaining approvals for the access to such data.

These regulations specifically address topics like the need to register applicable consideration with the CNBV and the obligation of "Data Providers" to report to such regulator any information security incidents, as well as the possibility of interrupting the sharing of data upon breaches by "Data Petitioners", and the requirements of compliance remediation (*regularización*) programs for entities to implement in response to violations of the regulations.

It is important to highlight that, pursuant to the CNBV Regulations, Data Petitioners will be deemed automatically approved by the CNBV, and thus enabled to access data from Data Suppliers to whom they apply for access, should they comply with certain requirements. Those requirements are contained in the three exhibits to the CNBV Regulations and basically consist of the use of the Hypertext Transfer Protocol Secure, digital certificates issued by specific entities and the HSTS (*HTTP Strict Transport Security*) protocol, as well as the identification of Data Petitioners, the mitigation of attacks or intrusions and the structure and construction of messages transferred via APIs.

As for Data Suppliers, in addition to complying with these requirements, they shall (i) clearly, precisely and in Spanish, through their website or any other electronic means of communication, disclose the process for Data Petitioners to access data via APIs and the consideration to be paid for such data, which consideration shall have been previously approved by the CNBV; and (ii) adopt information security policies for the protection of infrastructure and the confidentiality and integrity of data. Such policies shall, among other things, include the mechanisms for identifying and authenticating the staff responsible for handling APIs, the encryption of data, a vulnerability and penetration assessment program, mechanisms for the back-up and retrieval of data so as to mitigate interruption risks and the preservation of complete audit records.

This GT Alert does not apply to U.S. matters or laws, nor to any jurisdiction outside of Mexico.

Authors

This GT Alert was prepared by:

- Carlos R. Garduño | +52 55.5029.0053 | gardunoc@gtlaw.com
- Carlos M. Escandón | +52 55.5029.0062 | escandonc@gtlaw.com