# CHAPTER 16

# MEXICO

Luis Burgueno
Von Wobeser y Sierra, S.C.
Santa Fe, Centro de Ciudad,
Delegacion Alvaro Obregon, Mexico

## 16.01 Introduction

In Mexico, a civil law country where contract law is fundamentally governed by enacted statutes of law and where the role of jurisprudence is basically limited to the interpretation of the law and thus has virtually no influence in the creation and evolution thereof, the challenge of e-commerce translates into a multiple quest. First, it becomes necessary to amend the legal codes that govern contract formation, validity, and other aspects of contract law, and these codes were enacted more than 70 years ago.[1]

At the same time, however, it is necessary to ensure that any laws enacted on e-commerce preserve some degree of flexibility to accommodate the possibility of carrying out commercial transactions by new means of communication that likely will emerge.

The United Nations International Trade Law Commission (UNCITRAL) Model Law on Electronic Contracts of 1996 (the "1996 Model Law") and the UNCITRAL Model Law on Electronic Signatures of 2001 (the "2001 Model Law") have proven to be useful for lawmakers worldwide in that they offer a system to resolve the new problems posed by e-commerce.

Mexico was one of the early subscribers to the 1996 Model Law and the 2001 Model Law.[2]

---

1 The main legal codes governing commercial and private contracts, in general, the Federal Civil Code and the Code of Commerce, were enacted in 1928 and 1889, respectively.

2 As of 29 July 2004, only Mexico and Thailand had adopted the 2001 Model Law; see http://www.uncitral.org.

On 29 May 2000, several provisions of the Federal Civil Code, Code of Commerce, Federal Civil Procedure Code, and Federal Consumer Protection Act were amended[3] to legally recognize the validity and enforceability of contracts executed by electronic means, i.e., by the exchange of data messages, and the admissibility of data messages as evidence. The amendments (the "2000 E-Commerce Decree") incorporated only some of the basic principles of the 1996 Model Law, but they constituted a significant step towards full recognition of data messages and electronic signatures since they established the possibility of forming legally binding and enforceable contracts by electronic means.

On 29 August 2003, the Code of Commerce was amended[4] to regulate electronic signatures and to incorporate many provisions of the 1996 Model Law that had been left out of the 2000 E-Commerce Decree.

In the matter of electronic signatures, the second set of amendments to the Code of Commerce (the "2003 E-Signatures Decree") substantially follows the guidelines of the 2001 Model Law,[5] with some significant additions regarding the regulation of certification service providers.

This chapter presents Mexico's legal regime on electronic contracting and signatures, as has been established pursuant to the 2000 E-Commerce Decree and the 2003 E-Signatures Decree, and the manner in which the provisions of the UNCITRAL 1996 and 2001 Model Laws have been implemented. In addition, bearing in mind the current works of the UNCITRAL Working Group IV (Electronic Commerce) on a Draft Convention on the Use of Electronic Communications in International Contracts (the "Draft Convention"), this chapter also refers to some of the most significant differences between Mexican law on e-contracts and e-signatures and the Draft Convention.[6]

---

3 *Diario Oficial de la Federación*, effective 29 May 2000. Pursuant to transitory article 1 to of the Decree; the amendments became on 7 June 2000.

4 *Diario Oficial de la Federación*, 29 August 2003. Approved by the Chamber of Representatives on 26 November 2002 and by the Senate on 8 April 2003. Pursuant to transitory article 1 of the Decree, the amendments became effective on 27 November 2003.

5 The Congressional Commerce and Industrial Promotion Commission that issued the opinion (*dictamen*) on the basis of which Congress voted and eventually approved the 2003 E-Signatures Decree expressly recognized that one of the considerations in preparing the bill was to "basically adopt the Model Law of [UNCITRAL] since it gathers experiences and studies of all the countries of the world, under the auspices of [UNCITRAL]". "Dictamen de la Comisión de Comercio y Fomento Industrial, con proyecto de decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio (*firma electrónica*)", *Gaceta Parlamentaria*, Year VI, Number 1135, 21 November 2002; see http://gaceta.diputados.gob.mx/Gaceta/58/2002/nov/20021121.html.

6 For the purposes of this chapter, references to the Draft Convention refer to the UNCITRAL Working Group IV's revised draft version released on 18 May 2004, after the Working Group's 43rd session.

## 16.02 Electronic Commerce

### (a) In General

*(i) Sphere of Application*

The main body of law on electronic commerce has been incorporated into the Code of Commerce, specifically in Title 2 (of Electronic Commerce) of the Second Book (of Commerce in General). Most of the key provisions of the UNCITRAL 1996 and 2001 Model Laws have been implemented in Title 2, which is divided into four chapters, as follows:

1. Chapter I. On Data Messages;
2. Chapter II. On Signatures;
3. Chapter III. On Certification Service Providers; and
4. Chapter IV. On the Recognition of Foreign Certificates and Electronic Signatures.

The Code of Commerce being a federal statute, the provisions of Title 2 are applicable in all of Mexico in commercial matters, except as otherwise provided for by international treaties to which Mexico is or becomes a party.[7]

The reference to "commercial matters" implies a very extensive sphere of application. Under the Mexican Constitution, the Federal Congress is empowered to regulate commerce. Accordingly, the e-commerce law provisions contained in Title 2 should be applicable to all such matters legislated by the Federal Congress in exercise of this power, which include:

1. Acts of commerce;
2. Corporations and other business organizations; and
3. Negotiable instruments and credit transactions.

The concept of "acts of commerce" contained in article 75 of the Code of Commerce, which determines the scope of what constitutes commerce for legal purposes, is very broad and flexible. Article 75 lists an extensive, but not limited, catalogue of transactions that are deemed to be "acts of commerce", ranging from purchases and sales of movable and real estate property, leases of movable assets, purchase and sales of equity interests, bonds and other securities, to insurance, deposits, and credit transactions. Article 75 broadens the concept of acts of commerce by stating that any other acts that are "analogous" to those listed in the catalogue will be deemed to be acts of commerce.

---

7 Code of Commerce, article 89.

The Code of Commerce does not provide for exceptions to the applicability of Title 2 to commercial matters, despite the fact that the application of some provisions of Title 2 to some particular commercial matters may be found to be extremely problematic, especially in the case of negotiable instruments, that system being based on the principle that the holder's rights are deemed to be incorporated into the supporting paper. It remains to be seen how Mexican courts will apply the provisions of Title 2 to this area of commercial law.

Some of the basic concepts of the 1996 Model Law (i.e., the functional equivalence of data messages with written documents, the possibility of forming contracts by electronic means, and the recognition of data messages as evidence) have been incorporated directly into the Federal Civil Code and the Federal Code on Civil Procedure, which extends the application of these principles to all kinds of contracts and transactions that are subject to federal laws, whether or not they are deemed to be commercial.

Accordingly, while Title 2 is only applicable to commercial matters, the e-commerce provisions that were incorporated into the Federal Civil Code will have application beyond commercial matters. In addition, the Federal Consumer Protection Act was amended as part of the 2000 E-Commerce Decree to establish certain obligations of suppliers that carry out transactions with consumers by electronic means (see text, below.)

The provisions of Title 2 apply to both domestic and international transactions, when applicable conflict-of-laws provisions point to the application of Mexican Laws. Because Mexican law on conflict of laws follows the principle that, in contracts and other acts of will, form requirements are governed by the laws of the place of execution thereof,[8] the provisions of Title 2 will generally apply whenever the act of will or contract is deemed to have been executed in Mexico. In addition, Mexican Law provides that, when an act of will or contract will have legal effects in Mexico, the parties may choose to subject themselves to the formalities established in Mexican Laws.[9]

Mexico is a party to the Inter-American Convention on the Law Applicable to International Contracts, which was signed in 1994 and entered into force on 15 December 1996.[10] Accordingly, the provisions of Title 2 will be

8 Federal Civil Code, article 13(IV).

9 Federal Civil Code, article 13(IV).

10 The Inter-American Convention has been signed, *ad referendum*, by five countries (Bolivia, Brazil, Mexico, Uruguay, and Venezuela). Venezuela was the first country to deposit its ratification instrument with the Organization of American States (OAS). The Inter-American Convention entered into force, in accordance with article 18 thereof, 30 days after the second country, Mexico, deposited its ratification instrument with the OAS. See http://www.oea.org.

applicable to international contracts where, pursuant to the Inter-American-Convention, Mexican law is applicable.[11]

For this purpose, the Inter-American Convention allows the parties to a contract to agree on the applicable laws and, absent such agreement, follows the principle of "closest ties", which must be determined considering all relevant objective and subjective elements of the contract.[12]

Finally, reference should be made to the fact that the Code of Commerce establishes that the provisions of Title 2 will only apply "without prejudice to the international treaties to which Mexico is a party". This opens the way for the adoption and application by Mexico of international treaties on the e-commerce, such as the Draft Convention.

If Mexico becomes a party to the Draft Convention, it would become part of Mexican Law but, in case of conflict, the Draft Convention would prevail over Title 2. Nevertheless, even if the Draft Convention is adopted, Title 2 will still have a significant scope of application. Title 2 would still apply to:

1. E-commerce transactions that are not deemed to be international pursuant to the Draft Convention, i.e., where the contracting parties do not have their places of business in various states;
2. International e-commerce transactions that are excluded from the scope of application of the Draft Convention, and thus would still apply to transactions of great importance and frequency, such as (a) consumer transactions, (b) transactions on regulated exchanges, (c) real estate transactions, (4) negotiable instruments, and (5) documents related to the carriage of goods.[13] It should be noted that, at the time of writing, the UNCITRAL Working Group has not finalized its revision of this article, and it may add other exclusions to the sphere of application of the Draft Convention.
3. Where the contracting parties have agreed to exclude the application of the Draft Convention, and the applicable international private laws point to the application of Mexican law; and

---

11 The Inter-American Convention "determine[s] the law applicable to international contracts".

12 Inter-American Convention. article 9: "If the parties have not selected the applicable law, or if their selection proves ineffective, the contract will be governed by the law of the State with which it has the closest ties. The court will take into account all objective and subjective elements of the contract to determine the law of the State with which it has the closest ties . . . ").

13 Draft Convention on the use of Electronic Communications in International Contracts, article 2.

4. International e-commerce transactions subject to the Draft Convention, where a question is (a) not expressly settled in the Draft Convention, (b) not capable of being sold pursuant to the general principles in which the Draft Convention is based, and (c) the applicable rules of international private law point to the application of Mexican law.

*(ii) Definitions*

In the matter of e-contracting and e-commerce, in general, Mexican Law has incorporated the basic definitions contained in the 1996 Model Law, almost without change.[14]

"Data message" is defined as the information generated, sent, received, or stored by electronic or optical means or by any other technology. This definition is slightly different from that proposed by the 1996 Model Law in that the Model Law refers to "any other technology" rather than to "similar means". The change is clearly intended to cover any information technology, although its use is not very fortunate since the term "technology" can be, if read literally, applied to non-electronic means for generating, sending, receiving, or storing information.

"Intermediary of a data message" is defined as any person who, acting on behalf of another person, sends, receives, or stores such data message or provides another service in connection therewith.

"Originator of a data message" is any person who, pursuant to the data message, has acted on its own name or on whose behalf the data message was sent or generated before being stored, if applicable, but who has not acted as an intermediary.

"Addressee of a data message" is defined as the person designated by the originator to receive the data message, but who is not acting as an intermediary in connection with that data message.

"Information system" means any system used to generate, send, receive, store, or otherwise process data messages.

Significantly, Title 2 does not include a definition of "electronic data interchange", which is one of the many types of technologic means of communicating data messages.

These definitions are generally consistent with those of the 1996 Model Law and the Draft Convention, although there are many subtle changes that, when applied to concrete, real cases, may result in significant departures from their intended solutions. To cite an example, one can note that an addressee under Mexican Law is the person "designated" by the originator

14 These definitions are contained in article 89 of the Code of Commerce.

to receive the data message while, under the 1996 Model Law and the Draft Convention, the prevailing criteria is the originator's intention.

To "designate" implies an express indication of the identity of the addressee and is one way, but not the only one, to show or evidence intention. In light of this difference, in case of an erroneous designation of the intended receiver of the data message, under Mexican law, the addressee would still be the erroneously designated person, but not under the 1996 Model Law and the Draft Convention.

This chapter will not elaborate on such subtle differences, real effect of which can only be analyzed on a case-by-case basis and in a real-life context. Nevertheless, it is important to keep in mind the existence of these subtleties when attempting to apply the provisions of Mexican law to real cases, since they can result in different solutions to the same questions.

*(iii) Interpretation*

The application and interpretation of the provisions of Title 2 must be subject to the principles of technological neutrality, party autonomy, international compatibility, and functional equivalence of data messages in connection with information documented in non-electronic means and of the electronic signature in connection with an autograph or handwritten signature.[15]

In this regard, Mexican law differs from both the 1996 Model Law and the Draft Convention in many instances. It does not refer to its international origin or to the need to promote uniformity in its application, even though a vague reference is made to "international compatibility", which is not sufficient to support the position that Mexican courts would have to attempt to apply Title 2 in an internationally consistent manner.

While there is no express reference to the need to promote "the observance of good faith", it should be considered that the observance of good faith is a general principle of Mexican law and of commercial law in particular; thus, this change is not substantial.

Finally, Title 2 does not contain a provision that, as with article 3(2) of the 1996 Model Law and article 5(2) of the Draft Convention, establishes a gap-filling rule. This means that, in case of questions concerning e-commerce that are not expressly settled in Title 2, the general gap-filling rules of Mexican law, set out in article 14 of the Mexican Constitution and article 19 of the Federal Civil Code, would apply. Thus, a judge will attempt to solve the question by the letter of the law or its juridical interpretation. In the absence of a legal statutory provision, the judge will resolve the question by resorting to the general principles of Mexican law.

15 Code of Commerce, article 89.

*(iv) Variation by Agreement*

Title 2 does not contain a provision that, similar to article 4 of the 1996 Model Law and article 3 of the Draft Convention, expressly recognizes the parties' rights to contractually modify or exclude the applicability of its provisions to the relationships between them.

This absence should not, however, be interpreted as meaning that the parties cannot agree to different rules to be applicable to the exchange of electronic messages between them. The e-commerce laws contained in Title 2, as any other private law statutory provisions, can be amended or even derogated by agreement of the parties to the extent that they are not *ordre public* or public policy laws.

As a general principle, there will be a strong presumption that all the statutory provisions contained in Title 2 are private laws subject to amendment or derogation by the parties, given the general statement contained in article 89, pursuant to which the principle of party autonomy must govern the interpretation and application of the provisions of Title 2.

### (b) Application of Legal Requirements to Data Messages

*(i) Legal Recognition of Data Messages*

As a general principle, incorporated into Mexican law by the 2003 E-Signatures Decree, information will not be deprived of legal effects, validity, or enforceability only because it is contained in a data message.[16]

This principle, which is of fundamental importance, has been copied almost verbatim from the 1996 Model Law and is consistent with the Draft Convention. The only difference (the Model Law and Draft Convention refer to information "in the form of" and Title 2 to information "contained in" the data message) does not appear to have any relevance.

*(ii) Incorporation by Reference*

On the other hand, Title 2 does not contain a provision that incorporates article 5 *bis* of the 1996 Model Law, despite the fact that the UNCITRAL Commission had already adopted it before Mexico enacted the 2003 E-Signatures Decree. The whole issue is whether information simply referred to in, rather than contained in, the data message should be given the same treatment as contained information. It bears noting that the UNCITRAL Working Group IV has not yet added a similar provision to the Draft Convention, despite the fact that article 5 *bis* was incorporated into the 1996 Model Law in 1998.

16 Code of Commerce, article 89 *bis*.

While the addition would have provided desirable clarification, it is not necessary. To the extent that the existence and content of the information referred to, but not included, in the data message, as well as the relevant party's intention in connection therewith, can be ascertained and eventually proven, the fact that such information is contained in a file or media different from the data message should be irrelevant. On the other hand, however, it must be taken into consideration that, as a general principle of Mexican law, in order for a person to waive rights to which he would otherwise be entitled by operation of law, such waiver must be clear and unambiguous, in such a manner that there is no doubt regarding the right that is waived.[17]

This provision is relevant because it is applicable to rights arising from contracts that the parties may want to contractually modify or derogate in electronic transactions. While not necessarily the case, waivers of rights made through reference to information not contained in the data message itself may be found by a court not to be clear and unambiguous waivers of rights.

*(iii) Writing*

The principle of functional equivalence of data messages in connection with information documented in non-electronic means has been treated in paragraph 1 of article 93 of the Code of Commerce, pursuant to which:

> Article 93. When the law requires that acts, agreements or contracts must be made in written form, this requirement will be deemed to be complied with in the case of data messages, provided that information contained therein is kept integral and is accessible for further consultation, without regard to the format in which it is or is represented.

Article 93 presents one significant difference from article 6 of the 1996 Model Law and article 8 of the Draft Convention. In addition to accessibility, Mexican Law requires that the information contained in the data message maintain its integrity. This addition, while it may have been well intentioned, is unfortunate. Traditionally, legal requirements for contract formation, validity, and enforceability are determined and qualified by reference only to the time of execution of the contract, not afterwards.

On the other hand, article 93 appears to establish a requirement for contract formation that extends in time beyond the moment of execution thereof. The fact that some or even all of the information contained in a data message is destroyed or deteriorated after the execution of the agreement should not affect its equivalence to a written paper. A contract executed on paper is valid even if some or even all of the pages containing it are later destroyed or

17 Federal Code of Civil Procedure, article 7.

deteriorated.[18] Data messages should receive the same treatment in light of the functional equivalence principle.

Furthermore, under the Mexican law on contracts, a "written document" is equivalent to a "signed document" because written documents must be signed.[19] This is why the first paragraph of article 93 must be read together with the second paragraph thereof, which provides that:

> Article 93. Where in addition the law requires the signature of the parties, this requirement will be deemed to have been met in the case of data messages, provided that they are attributable to such parties.

A data message, from the perspective of the law, is equivalent to a written document, provided that three conditions are met, namely:

1. Integrity of the information contained therein;
2. Accessibility for further consultation; and
3. Attributability to the party.[20]

As mentioned above, legal recognition of data messages as equivalent to written documents has been incorporated in Mexico not only for commercial matters, but also for federal civil matters, by their inclusion in the Federal Civil Code. In this regard, article 1834 *bis* of the Federal Civil Code (added pursuant to the 2000 E-Commerce Decree) establishes that the written format requirements established by the Civil Code can be met by using "electronic or optical means or any other technology", provided that the information "generated or communicated in its integrity" by electronic means is attributable to the obliged person and accessible for further consultation.

It bears noting that article 1834 *bis* of the Civil Code limits the "integrity" requirement to the communication of the information, not to its preservation or maintenance over time. This solution appears more reasonable and technical than that of the Code of Commerce.

---

18 Obviously, this can create great problems for the relevant parties since it may be impossible to prove the execution of the agreement or the terms and conditions thereof without the original or at least a copy of the signed contract. Difficult, however, is not impossible. In addition, in some instances, both parties may be interested in recognizing the existence and terms and conditions of the executed agreement despite the destruction or deterioration of the paper on which it was documented.

19 This results from article 1834 of the Federal Civil Code, applicable to all types of acts of will, agreements, or contracts; it provides that "[w]hen written form is required for a contract, the relative documents must be signed by all persons to whom the law imposes such an obligation. If one of them cannot or does not know how to sign, someone else must sign the document on request, and the fingerprint of the person who did not sign must be printed in the document".

20 Kraft, *La Firma Electrónica y las Entidades de Certificación* (2003), at pp. 3–7.

On the other hand, Mexican Law has moved beyond the 1996 and 2001 Model Laws and the Draft Convention by establishing the possibility of using electronic communications to negotiate and execute legal acts or contracts that, pursuant to the law, are required to be executed in a public deed or notarial act. Pursuant to article 93 of the Code of Commerce,[21] where the applicable law establishes such a requirement, the authenticating officer (notary public or public broker in most instances) and the contracting parties may use data messages to establish the "exact terms" pursuant to which they are willing to be obliged. The participating officer must:

1. Expressly set forth, in the public deed or act, the elements pursuant to which the messages are attributed to the contracting parties;
2. Keep under his custody an integral version of the data messages for further consultation; and
3. Issue public instruments pursuant to the applicable laws.

It is significant that Title 2 still requires that the public deed or instrument be issued "pursuant to the applicable laws", and this has a double implication. First, Title 2 still requires that the public instrument be issued, while it facilitates the negotiation and execution process by not requiring the presence of the parties before the authenticating officer for the "signature" of the public deed. Second, Title 2 recognizes that notaries public, the most important type of authenticating officers, are regulated by state rather than federal laws; thus, there are limitations as to what the Code of Commerce (being a federal statute) can regulate regarding the notary public function.

In contrast to the 1996 Model Law and the Draft Convention, there is no statutory provision in Mexican Law stating that this principle is applicable, irrespective of whether the written form requirement is expressed as an obligation or by establishing certain consequences in case such written form is missing. Nevertheless, interpreted correctly, the provisions of article 93 should be applicable, irrespective of the manner in which the written form requirement is expressed, particularly in light of the fact that article 89 mandates that the provisions of Title 2 be interpreted pursuant to the principle of functional equivalence of data messages in connection with other documents.

*(iv) Signature*

**In General** As mentioned above, for a data message to be equivalent to a written document, which under Mexican Law and for contract formation purposes means a written and signed document, the data message will be

21 Federal Code of Civil Procedure, article 1834 *bis*, contains the same provision, with some insignificant language differences.

attributable to the relevant party, i.e., to the person that, had it been a paper document, should have signed it.

One of the means for achieving this purpose is by the use of electronic signatures. As described above, Mexico has incorporated most of the provisions of the 2001 Model Law into Title 2 of the Code of Commerce.

**Sphere of Application** Being part of Title 2 of the Code of Commerce, the statutory provisions of law on electronic signatures have the same sphere of application described above in connection with Title 2 and e-commerce law provisions in general.

**Definitions** Title 2 contains several definitions of terms related to e-signatures that generally follow the definitions proposed by the 2001 Model Law. These definitions are the following:

"Electronic signature" is defined as the electronic data contained in a data message, or attached or logically associated thereto by any technology, which is used to identify the signatory in relation to the data message and to indicate that the signatory approves the information contained in the data message, and produces the same legal effects as the autograph signature, it being admissible as evidence in court. This definition is substantially identical to that of the 2001 Model Law, except for the fact that Mexican law emphasizes:

1. Its equivalence with handwritten signatures as to their legal effects; and
2. Its admissibility as evidence in litigation.

"Advanced Electronic Signature" or "Reliable Electronic Signature" is defined as that electronic signature that complies with the requirements set forth in parts I–IV of article 97. This definition was added by Mexican law for practical purposes and, although it has no equivalent in the 2001 Model Law, the underlying concept is not new.

Parts I–IV of article 97 of the Code of Commerce describe those requirements that, if met by an electronic signature, are sufficient to consider it reliable for purposes of satisfying the legal requirement of a signature. These four requirements are substantially similar to those established in section 6(3)(a)–(d) of the E-Signature Model Law in connection with electronic signatures that are "considered to be reliable" for the purposes of substituting for a written signature (see text, below).

"Signatory" means the person who possesses the signature creation data and who acts in his own name, or in the name of the person whom he represents.

"Relying party" means the person who, whether or not the addressee, acts on the basis of a certificate or an electronic signature.

"Certificate" means any data message or other record which confirms the connection between the signor and the electronic signature creation data.

"Electronic signature creation data" is the unique data, such as private cryptographic codes or keys, which the signatory generates secretly and uses to create his electronic signature to ensure the connection between the electronic signature and the signatory. This definition was added by Mexican Law and has no equivalent in the 2001 Model Law or the Draft Convention.

"Certification services provider" means the person or public institution that renders services related with electronic signatures and who issues certificates.

**Treatment of Signature Technologies** The provisions of Title 2 are to be applied in such a manner that they do not exclude, restrict, or deprive from legal effects any method to create an electronic signature.[22] This provision substantially reproduces article 3 of the 2001 Model Law.

It does not, however, make an express reference to the parties' right to agree otherwise (i.e., to derogate or vary the effects of e-signature laws) contained in article 5 of the 2001 Model Law, probably because article 5 was not copied into Title 2. As noted, this should not be interpreted as *per se* limiting or restricting the parties' ability to contractually modify or derogate the effect of the e-signature provisions of Title 2.

**Interpretation** The interpretation provisions of Title 2, as described above, also are applicable in the matter of e-signatures. Accordingly, in the interpretation and application of the e-signature provisions contained in Title 2, the principles of technological neutrality, party autonomy, international compatibility, and functional equivalent of electronic signature in connection with written signatures will govern.[23]

**Variation by Agreement** There is no provision in Title 2 expressly establishing the parties' rights to contractually derogate or amend the effects of the legal provisions applicable to e-signatures.

Nevertheless, considering the general principles of Mexican law (i.e., parties can derogate or amend the effects of private law provisions to the extent not contrary to public policy) and the legislators' mandate to interpret and apply these provisions in light of the party-autonomy principle, it should be considered that all the provisions regarding electronic signatures contained in Title 2 are subject to contractual derogation or modification.

Mexican law establishes that an electronic signature must be "appropriate" rather than "reliable as appropriate", as proposed by the 2001 Model Law,

22 Code of Commerce, article 96.

23 Code of Commerce, article 89.

article 6(1). Nevertheless, this difference does not appear to have any significant consequence since, as will be shown, Title 2 focuses the qualification of electronic signatures on their "reliability".

Following article 6(3) of the 2001 Model Law in all substantial respects, Title 2 establishes that an electronic signature is to be considered advanced or reliable if the following minimum requirements are met:

1. The electronic signature creation data, within the context in which they are used, correspond exclusively to the signatory;
2. The electronic signature creation data were under the exclusive control of the signatory at the moment of the signing;
3. It is possible to detect any alteration to the electronic signature made after the signing; and
4. It is possible to detect any alteration to the integrity of the data message made after the signing.

The fulfillment of these four requirements provides a presumption that the electronic signature is reliable. The reliability of the electronic signature, however, can be proved by any other means by an interested party and, on the other hand, a party may rebut this presumption by adducing evidence that the electronic signature is not reliable.

As in the case of the written form requirement, and different from the 2001 Model Law, article 6(s), and the Draft Convention, article 3, there is no statutory provision stating that electronic signatures can substitute hand written signature, irrespective of whether the signature requirement is expressed as an obligation or by establishing certain consequences in case such signature is missing.

Again, the principle of functional equivalence of electronic signatures in connection with autograph signatures incorporated as a governing principle of interpretation of the provisions of Title 2 should lead to consider that the provisions of article 97 are applicable, irrespective of the manner in which the signature requirement is established.

**Conduct of Signatory** In using electronic signatures, the signatory must comply with several obligations listed in article 99 of the Code of Commerce. If the signatory fails to comply with these obligations when due, he will be liable for all legal consequences arising therefrom. The obligations established by article 99 are the following:

1. The signatory must comply with the obligations arising from the use of the electronic signature;[24]

24 Code of Commerce, article 99(I).

2. The signatory must act diligently and establish reasonable means to avoid the unauthorized use of the electronic signature creation data;[25] and
3. When using a certificate in connection with an electronic signature, the signatory must conduct himself with reasonable diligence must ensure the exactitude of all representations made in connection with the certificate or its term or that have been included in the certificate.[26]

Article 99 does not reproduce the provisions of article 8(1)(b) of the 2001 Model Law regarding signatories' obligation to inform the addressee and potential reliant parties of the actual or potential compromise of the electronic signature creation data. However, it is clear that, if the signatory is aware of this circumstance, failure to so inform the addressee (or other potential relying parties, will be considered as a negligent act on its part, and thus must comply with the obligations arising from the unauthorized use.

**Certification Service Providers** Certification service providers are heavily regulated under Mexican law. Title 2 devotes chapter 3 to regulating who can operate as a certification service provider, the requirements that must be met and authorizations that should be obtained, their obligations and liabilities, and the characteristics of the certificates they issue.

On 19 July 2004, the Regulations of the Code of Commerce on the Matter of Certification Service Providers were enacted, and they detail many of the provisions of chapter 3, particularly regarding the requirements to operate as a certification service provider and its administrative obligations.

The Secretariat of Economy (*Secretaría de Economía*) is entrusted with enforcing the statutory provisions and with enacting complementary regulations.

*Accreditation* Notaries public[27] and public brokers,[28] private legal entities, and public institutions can operate as certification service providers, provided that they previously obtain from the Secretariat an authorization, which is referred to as "accreditation".

---

25 Code of Commerce, article 99(II). If the signatory does not act diligently in this regard, he must comply with the obligations arising from the unauthorized use of his signature, unless the addressee actually knew that the electronic signature was not secure or the addressee did not himself act diligently. Code of Commerce, article 99(IV).

26 Code of Commerce, article 99(III).

27 Mexican law establishes a civil law notary system.

28 Under Mexican Law and practice, "public brokers" have functions similar to civil law notaries, but limited to commercial transactions.

The ability to issue certificates does not grant, by itself, public faith[29] or authentication power, i.e., the power granted by the state to notaries public, public brokers, and some governmental officers to certify, with full evidentiary weight, the authenticity (and, in some instances, legality) of acts to which they attest.

With this in mind, Title 2 expressly establishes that notaries public and public brokers can issue certificates that involve public faith or not, and that these certificates can be issued in paper documents, electronic files, or any other media that may store information. The Secretariat is obliged to grant the accreditation, provided that the applicant has:

1. Filed an application for accreditation as a certification service provider;
2. The human, material, economic, and technological resources required to provide the service and to guarantee the security of the information and its confidentiality;[30]
3. Defined and specific procedures for the processing of certificates and measures that ensure the seriousness of the issued certificates and the maintenance and consultation of the records;
4. Provided assurances that the individuals who operate or have access to the certification systems of the certification service provider have not been convicted of a crime against patrimony (such as robbery or fraud) or which has been punished with imprisonment, or been disqualified, for any reason, to practice their profession or to occupy a position in the public service or the financial system or to engage in commerce;
5. Contracted for a guaranty bond for the amount and subject to the conditions established in the regulations issued by the Secretariat;
6. Agreed, in writing, to be audited by the Secretariat; and
7. Registered its certificate with the Secretariat.

In addition, the corporate purpose of private legal entities must meet certain requirements.[31]

Financial institutions and companies that provide services to financial institutions in connection with fund or securities transfer also will be subject to the statutory provisions applicable thereto, as well as to the additional regulations issued by the relevant regulatory agencies.[32] If the Secretariat

29 Code of Commerce, article 100.

30 Regulations on Certification Service Providers, article 5(III).

31 Code of Commerce, article 101, requires that the corporate purpose of legal entities must authorize them to carry out certain activities, such as verifying the identity of users and the integrity and sufficiency of data messages and verifying electronic signatures.

32 Code of Commerce, article 106.

does not reject or otherwise rules on the application within 45 days of filing, the accreditation is deemed to have been granted.

*Obligations* Certification service providers must comply with several obligations established in Title 2. Failure to comply with such obligations by certification service providers may result not only in civil or criminal liability, but also in administrative liability. The Secretariat may, depending on the circumstances, temporarily or permanently suspend a certification service provider's authorization to operate as such.[33]

The most significant obligations of certification service providers are described below. While they are generally consistent with the 2001 Model Law and the Draft Convention, the regime established by Title 2 is exhaustive, and it contains many provisions that could be considered to be administrative law or regulation and which thus exceed or fall beyond the purposes of both the 2001 Model Law and the Draft Convention.

In addition to obtaining the prior accreditation from the Secretariat, certification service providers must notify the Secretariat of the beginning of their certification services activities within 45 days.[34]

The first obligation of certification service providers is to determine and inform to their users whether or not the electronic signatures they offer comply with the requirements set forth in Title 2 to be considered as advanced or reliable electronic signatures.[35] Such determination must be made in a manner which is compatible with standards and criteria that are internationally recognized.[36]

In addition, certification service providers must comply with several operations-related obligations, many of which are in addition to those established in article 9 of the 2001 Model Law. These obligations, set forth in article 104 of the Code of Commerce, are the following:

1. Verify, by themselves or through an individual or legal entity acting in its name and on its behalf, the identity of the applicants and any circumstances that are relevant for the issuance of the certificates, using any legally admitted means, provided that they are previously notified to the applicant;
2. Make available to the signatory the means for generating the creation data and verifying the electronic signature;

---

33 Code of Commerce, articles 110, 111, and 112. If a certification service provider looses its accreditation, the registry of certificates and certificates issued by it will be transferred to a another accredited certification service provider.

34 Code of Commerce, article 102.

35 Code of Commerce, article 98.

36 Code of Commerce, article 98.

3. Inform to the person requesting its services, prior to the issuance of the certificate, of its price, of the precise conditions for the use of a certificate, of its limitations of use and, if applicable, of the manner in which it guarantees its potential liability;
4. Maintain a registry of issued certificates which must record the issued certificates and include the circumstances affecting the suspension, loss, or expiration of their effects;[37]
5. Maintain confidentiality in connection with the information received to provide the certification services;[38]
6. Ensure the means to avoid the alteration of the certificates and to maintain the confidentiality of the data in the process of generating the electronic signature creation data;
7. Make information on its standards and practices available to the user and the addressee; and
8. Provide access means that enable the relying party to determine (a) the identity of the certification service provider, (b) that the signatory identified in the certificate had control over the device and electronic signature creation data when the certificate was issued, (c) that the electronic signature creation data were valid on the date when the certificate was issued, (d) the method used to identify the signatory, (e) any limitation on the purposes or the value in connection with which the electronic signature creation data or the certificate may be used, (f) any limitation regarding the certification service provider's liability, (g) whether there is a way for the signatory to inform the certification service provider that the electronic signature creation data have been somehow compromised, and (h) if a service of termination of the effectiveness of the certificate is offered.

Failure by a certification service provider to comply with these obligations can be sanctioned by the Secretariat, even by suspending, permanently or temporarily, its ability to provide certification services.[39] This is in addition to any civil or criminal liability which the certification service providers may incur.[40]

---

37 The registry may be available by electronic, optical, or any other means or technology, and its public content must be available to persons who so request; the private content must be available to the addressee and to persons who so request and who are authorized by the signatory, and in other cases set forth by the applicable laws and regulations.

38 If the certification service provider ceases its activity, it must notify the Secretariat to determine, pursuant to the applicable regulations, the destiny of its registries and archives.

39 Code of Commerce, article 110.

40 Code of Commerce, article 111.

**Validity and Expiration of Certificate** Mexican law establishes requirements that certificates must meet for them to be valid as such. There is no similar provision in the 2001 Model Law or the Draft Convention, which generally do not regulate the contents of certificates.

Article 108 of Title 2 establishes that, in order for a certificate to be valid, it must contain the following:

1. The indication that it is issued as a certificate;
2. The exclusive identification code of the certificate;
3. The identity of the certification service provider that issued the certificate, its corporate name, address, email address, and the Secretariat's accreditation data;
4. The name of the certificate's title holder;
5. The term of the certificate;
6. The date and hour of the certificate's issuance, suspension, or renovation;
7. The scope of the responsibilities assumed by the certification service provider; and
8. The reference to the technology used to create the electronic signature.

The addition and language of article 108 are very unfortunate. Article 108 creates more problems than it solves, particularly since Title 2 also imposes on addressees and relying parties the obligation to verify the "validity" of certificates (see text, below), In addition, article 108 treats all requirements as equally important (failure to comply with any of them results in invalidation), and it does not attempt to provide any solutions in case of omission.[41]

Pursuant to article 109, a certificate will no longer be effective in any of the following cases:

1. The term of the certificate has expired, unless it has been renewed by the signatory;[42]
2. The certificate has been revoked by the certification service provider, on the request of the signatory, the legal entity represented by the signatory, or an authorized third party;
3. The device containing the certificate is lost or becomes unusable;

41 There are no solutions by default as, e.g., a default term of one year would be.

42 The term of the certificate cannot exceed two years from the date of issue.

4. It is established that, at the time of its issuance, the certificate did not comply with the requirements established by law;[43] or
5. A court or competent authority issues a resolution ordering termination.

The termination of effectiveness, however, applies only to the future, and it does not affect the rights of persons who acted in reliance thereon while the certificate was still valid. These provisions have no equivalent in the 2001 Model Law or the Draft Convention.

**Trustworthiness** There is no stand-alone statutory provision similar to article 10 of the 2001 Model Law that establishes the criteria that must be met for the systems, procedures, and human resources utilized by a certification service provider.

Nevertheless, the dense body of regulation contained in chapter III of Title 2 regarding certification service providers (see text, above) is clearly intended to ensure the trustworthiness of the certification services and generally complies with, and in some instances exceeds, the standards set forth by article 10 of the 2001 Model Law.

Most of the "factors" listed in article 10 of the 2001 Model Law as available means of ensuring the trustworthiness of a certification service provider are dealt with by other statutory provisions of Title 2, even if in a different and sometimes stricter manner.

For instance, the 2001 Model Law's "regularity and extent of audit by an independent body" factor is covered in Title 2 by the requirement that, when applying for an accreditation to act as a certification service provider, the applicant must agree in advance to be audited by the Secretariat.

In connection with the "financial and human resources, including existence of assets" in article 10(a) of the 2001 Model Law, Title 2 establishes that, to obtain the accreditation, the applicant must have:

> . . . the human, material, economic, and technological resources required to provide the service, to guarantee the security of the information and its confidentiality.[44]

In other instances, these factors have been reflected in the Regulations on Certification Service Providers, which detail the requirements that must be met to be accredited and operate as a certification service provider.

**Conduct of Relying Party** Following in all substantial respects the provisions of article 11 of the 2001 Model Law, Title 2 imposes on the addressee

---

43 Such situation will not affect the rights of third parties acting in good faith.

44 Code of Commerce, article 102(A)(II).

and the relying party the obligation to take reasonable steps to verify the reliability of the electronic signature and its supporting certificate.

Accordingly, pursuant to article 107 of the Code of Commerce, the addressee and, if applicable, the relying party will bear the legal consequences of their failure to take reasonable steps to:

1. Verify the reliability of the electronic signature; or
2. Where the electronic signature is supported by a certificate, verify, even immediately, the validity, suspension, or revocation of the certificate and observe any limitation of use contained in the certificate.

**Recognition of Foreign Certificates and Electronic Signatures** In connection with the recognition of foreign certificates and electronic signatures, Title 2 follows, almost verbatim, the principles set forth in article 12 of the 2001 Model Law. In general, Mexican law adopts the principle that, in recognizing legal effects to foreign certificates or electronic signatures, only their reliability is relevant.

Accordingly, in determining whether and to what extent a certificate or electronic signature produces legal effects, the following aspects should not be considered:

1. The place of issuance of the certificate;
2. The place of creation or use of the electronic signature; and
3. The place where the certification service providers or the signatory has its establishment.

A certificate issued outside Mexico will have the same legal effects in Mexico as a certificate issued in Mexico if it offers a level of reliability equivalent to that established in Title 2. An electronic signature created or utilized outside Mexico will have the same legal effects in Mexico as an electronic signature created or utilized in Mexico if it offers an equivalent degree of reliability.

To assess the "equivalent degree of reliability" requirement, international standards recognized by Mexico and any other relevant means of evidence will be regarded. It bears noting that, in contrast to the 2001 Model Law, the Code of Commerce uses the term "international standards recognized by Mexico" rather than "recognized international standards".

Finally, Title 2 again recognizes the prevalence of party autonomy by establishing that, if the parties agree to use between themselves certain types of electronic signatures and certificates that, agreement will be recognized sufficient for the purposes of crossborder recognition, unless that agreement is not valid or enforceable under the applicable law.

*(v) Original*

**In General** If the law requires that any information be presented and retained in its original form, this requirement will be deemed to be have been complied in connection with a data message if:

1. The information in the data message is preserved in its integrity; and
2. The data message can be shown or displayed if so required.[45]

**Integrity** Regarding integrity, and consistent with the 1996 Model Law, Mexican law requires that there must be a "reliable assurance" that the integrity of information has been preserved, from the moment it was generated in its definitive form, whether as a data message or in any other form.

The content of a data message is deemed to have preserved its integrity if the data message content has remained complete and unaltered, irrespective of the changes that the media containing it may have suffered as a result of the communication, storage, or display process. Mexican law in this point differs from the 1996 Model Law in that:

1. It does not make reference to the addition of endorsements; and
2. It refers only to changes in the "media" that contains the data message.

It is unclear whether by "media" the law refers to the "physical" media in which the information is stored (i.e., magnetic or optical disks or other memory devices) or to the electronic file embodying the data message. Nevertheless, bearing in mind that it refers to changes resulting from the "communication, storage, or display" of the media, article 93 *bis* in this regard should be interpreted as referring to the file containing the data message.

The required standard or degree of reliability will be determined in conformity with the purposes for which the information was generated, as well as all the relevant circumstances.

**Capability of Being Displayed or Shown** Title 2 also establishes that, if it is required by law that the information contained in the data message be presented, the information, in addition to being maintained as integral and unaltered from the moment it was generated in its definitive form,[46] must be capable of being displayed to the person to whom it is to be presented.

Article 49 of the Code of Commerce and article 210-A of the Federal Civil Procedure Code, which were added pursuant to the 2000 E-Commerce Decree but not amended by the 2003 E-Signatures Decree, require, in addition to the capability of being displayed, that the information contained in

45 Code of Commerce, article 93 *bis*.

46 Code of Commerce, article 49.

the data message be accessible for further consultation, a requirement that is not established in the 1996 Model Law. These requirements, however, should be deemed to be equivalent in most cases since it is unlikely that any circumstance will arise where a data message is accessible for consultation but cannot be displayed.

*(vi) Admissibility and Evidentiary Weight of Data Messages*

As part of the 2000 E-Commerce Decree, several provisions of procedural law statutes were amended to expressly admit data messages as evidence in litigation.

Article 1205 of the Code of Commerce (which contains the rules of procedure applicable to litigation involving commercial matters) was amended to include data messages among the types of admissible evidence. Article 1205, as amended, reads as follows:

> Article 1205 — Any and all elements that may produce conviction in the adjudicator's mind in connection with disputed or doubtful facts are admissible as evidence, and thus the parties', third parties' and expert declarations, public or private documents, judicial inspection, photographs, facsimiles, cinematographic, video and audio tapes, data messages, reconstructions of facts and, in general, any other similar thing or object that is useful to find out the truth will be taken as evidence.

The general principle (i.e., that any element suitable of producing conviction on disputed facts will be admitted as evidence) already existed under Mexican law so that an argument could have been made that data messages should have been recognized as evidence before the 2000 E-Commerce Decree, although express recognition is clearly helpful. In addition, notwithstanding that this provision was enacted in 2000, it also will apply to data messages generated prior to the enactment of the 2000 E-Commerce Decree that are adduced as evidence in court after 2000.

In connection with the evidentiary weight of data messages, and consistent with the general principles of Mexican law, a judge is granted broad discretion in weighting the evidence consisting of data messages. A key guideline is given by the legislator, i.e., the judge should consider the reliability of the method used to generate, store, communicate, or keep the data message. Article 1298-A of the Code of Commerce, also added pursuant to the 2000 E-Commerce Decree, reads as follows:

> Article 1298-A — Data messages are recognized as evidence. To assess the evidential weight of data messages, the reliability of the method pursuant to which it has been generated, stored, communicated, or retained shall be principally estimated.

The provisions of the Code of Commerce described above apply only to commercial procedure. To make them applicable to procedures of a civil

nature, the Mexican Congress added an article 210-A to the Federal Civil Procedure Code. It incorporates the same principles for civil procedures before federal courts.

*(vii) Retention of Data Messages*

Merchants are obliged to retain, for a minimum of 10 years, the originals of data messages in which contracts, agreements, or other commitments creating rights and obligations are consigned.[47] This obligation already existed in connection with merchants' correspondence and other documents but, after 2000, it was extended to data messages. Ten years is the maximum statute of limitations for civil and commercial matters.

In addition, article 49 of the Code of Commerce establishes that, for the purposes of retention and presentation of originals consisting of data messages, it is required that the information be maintained in its integrity and be accessible for further consultation.

Finally, the Code of Commerce empowers the Secretariat to issue the official standards (*Norma Oficial Mexicana*) that establish the requirements that must be complied with to retain data messages.

Mexican law in this regard differs from the 1996 Model Law in that there is no provision like article 10 thereof, which allows compliance with the requirement of retaining "documents, records, or information" by retaining data messages, subject only to certain conditions (accessibility, appropriate format, and sufficiency of identification of origin, destination, date, and time of sending and receipt).

### (c) Communication of Data Messages

*(i) Formation and Validity of Contracts*

Electronic and optical means, and any other technology,[48] can be used in acts of commerce and the formation thereof.[49] Moreover, data messages can be used to negotiate and execute any type of contracts subject to federal laws, since this principle has been adopted directly into the Federal Civil Code.

Pursuant to the 2000 E-Commerce Decree, it was recognized that consent can be expressed by data messages, in which case it is deemed to be a form of "express", rather than tacit or implicit consent.[50]

---

47 Code of Commerce, article 49.

48 As noted above, references to "any technology" should be interpreted as being made to any electronic or similar information technology.

49 Code of Commerce, article 89.

50 Federal Civil Code, article 1803.

Before the 2000 E-Commerce Decree, Mexican law expressly recognized the possibility of executing contracts by telecommunications means, particularly by telephone and telegraph. In the case of telegrams, however, it is required that, prior to entering into the agreement, the parties have entered into a contract agreeing to the execution of contracts by the exchange of telegrams and that the originals of the telegrams contain the signature of the contracting parties and the "conventional signs" (i.e., keys, codes, or passwords) established between them.

The 2000 E-Commerce Decree excluded data messages from this requirement by providing that offers to contract and acceptances thereof can be made by data messages without a prior agreement in this regard being required. The 2000 E-Commerce Decree did not, however, derogate this pre-contract requirement for telegrams, despite the fact that they are data messages pursuant to the 1996 Model Law and arguably under the definition of data messages of Title 2.

Also as part of the 2000 E-Commerce Decree, another principle was incorporated into the Federal Civil Code. Where an offer to contract is made by data messages, and no term has been set by the offeror for its acceptance, the offer expires if not accepted immediately, if the technology used allows the expression of offer and acceptance in an immediate form.[51]

From this provision, a conclusion can be drawn that, under Mexican law, contracts executed by exchanging data messages will be subject to the same rules as contracts negotiated face to face or by telephone, to the extent that the technology used allows for the immediate communication of offer and acceptance, such as on-line communications. On the other hand, if the technology used does not so allow (as in the case of fax or email), the contract formation process should be subject to the rules applicable to the execution of contracts between distant parties (*entre ausentes*) or by correspondence.

Finally, the Code of Commerce provides that commercial contracts executed by electronic means are perfected on receipt of the acceptance to an offer or proposal to contract or the acceptance to the conditions on which an offer was amended.[52]

While these provisions differ from the 1996 Model Law, they follow its guiding principles, and they should be regarded as a way of implementing the provisions of the 1996 Model Law into the Mexican legal system.

---

51 Federal Civil Code, article 1805.

52 Code of Commerce, article 80.

*(ii) Recognition by Parties of Data Messages*

There is no provision in Title 2 or the Code of Commerce that, similar to article 12 of the 1996 Model Law, expressly establishes that declarations of will and other statements contained in data messages should not be deprived of legal effects only because they are in the form of data messages.

Nevertheless, considering the general legal recognition of data messages (see text, above) and the provisions that expressly recognize that data messages can be used in the formation of acts of commerce[53] and contracts in general,[54] this principle should be seen to be incorporated into Mexican law.

*(iii) Attribution of Data Messages*

**In General** Mexican law establishes a complex system of presumptions to determine whether a data message is attributable to the originator which, although generally following the structure and guidelines of the 1996 Model Law, differs in its final result.

**Presumed Precedence of Data Message** Article 90 of the Code of Commerce provides that a data message will be presumed to proceed from the originator if it has been sent:

1. By the originator itself;
2. By a party using the originator's identification means, such as keys or passwords;
3. By a person authorized to act in the name of the originator in connection with that data message; or
4. By an information system programmed by the originator or in its name to operate automatically.

Three of these four cases are taken from the 1996 Model Law, article 13(1) and (2), while the presumed attribution by the use of the identification means of the originator is not. The main problem in this regard is that, by establishing these rules as presumptions, and pursuant to the general principle that any presumption is rebuttable unless the statutes expressly provide otherwise or when the effect of the presumption is to nullify an act or to deny an action,[55] a person may adduce evidence to deny the attribution of the data message to its originator, even if it is proved that it was sent by him.

---

53 Code of Commerce, article 89.

54 Federal Civil Code, article 1803.

55 Code of Commerce, articles 1281 and 1282.

**Presumed Sent by Originator** In connection with the above, and to evidence that the data message has been sent by the originator itself, Title 2 establishes a second presumption in article 90 *bis*, which basically follows the provisions of 1996 Model Law, article 13(3) and (4). A data message is presumed to have been sent by the originator and, therefore, the addressee or the relying party can act accordingly, if:

1. The addressee or relying party has adequately applied the proceeding agreed to in advance with the originator, to establish that the data message actually proceeded from the originator; or
2. The data message received by the addressee or the relying party results from the action of an intermediary, to whom access has been given to a method used by the originator, to identify a data message as its own.

Nevertheless, the addressee or the relying party will lose the right to act in reliance of this presumption from the moment that any of the following occur:

1. The addressee or relying party has (a) been informed by the originator that the data message did not proceed from him and (b) had a reasonable period of time to act accordingly;[56] or
2. The addressee or relying party knows, or should have known by acting with due diligence or by applying an agreed method, that the data message did not come from the originator.

In connection with this, yet another presumption is established in favor of the addressee or relying party. It will be presumed that they acted with due diligence if the method used by the addressee or relying party complies with the requirements established by the Code of Commerce to verify the reliability of electronic signatures. This presumption, however, is rebuttable (i.e., a party affected by this presumption can submit evidence to prove otherwise) and not exclusive (i.e., the addressee or relying party can prove their due diligence by other means).

Finally, Title 2 does not incorporate the provisions contained in the 1996 Model Law's article 13(5), regarding error in communications, and (6), regarding duplicity of data messages.

*(iv) Acknowledgment of Receipt*

The originator can, prior to or at the moment of sending the data message, require or agree with the addressee that receipt of the data message must be

56 The statute does not define what constitutes a "reasonable period of time" in this context; thus, it will have to be determined on a case-by-case basis, considering all relevant circumstances.

acknowledged. The effects of such requirement or agreement in connection with the data message depend on whether or not the originator has indicated that the effects of the data message are conditional on the receipt of the acknowledgment, as described below.

If the originator has indicated that the effects of the data message are conditional on the receipt of the acknowledgment of receipt, the data message will be deemed not to have been sent if the acknowledgment of receipt is not received within the term set forth by the originator or within a term after the sending of the data message which is reasonable, considering the nature of the transaction.[57]

If the originator has requested or agreed with the addressee that receipt of the data message must be acknowledged, irrespective of the indicated form or method of acknowledgment, but the originator did not indicate expressly that the effects of the data message are conditional on the reception of the acknowledgement, and the acknowledgment has not been received within the requested or agreed term (or, if no such term exists, within a reasonable term, considering the nature of the transaction), the originator is entitled to give notice to the addressee, stating that the acknowledgement has not been received, and to specify a new reasonable term to receive it, which new term will be counted from the moment of this notice.[58]

Once the addressee's acknowledgement of receipt is received by the originator, it is presumed that the addressee has received the corresponding data message.[59]

The originator and addressee can agree on the form or method to be used to acknowledge receipt of the data message. If there is no agreement in this regard, the addressee is entitled to acknowledge receipt by:

1. Any communication from the addressee, automated or not; or
2. Any conduct of the addressee "that is sufficient to indicate to the originator that the data message has been received".[60]

All of these rules are substantially the same as those contained in article 14 of the 1996 Model Law.

*(v) Time and Place of Dispatch and Receipt of Data Messages*

**In General** Title 2 establishes, following the principles of the 1996 Model Law, a set of rules to determine the time when and place where a data message will be deemed to be dispatched or sent.

57 Code of Commerce, article 92(II).

58 Code of Commerce, article 92(III).

59 Code of Commerce, article 92(III).

60 Code of Commerce, article 92(I).

**Time** Articles 91 and 92 of the Code of Commerce set forth the rules applicable to determine when a data message has been dispatched and received. The rules can be amended by agreement between originator and addressee, or implicitly, if the effects of the data message have been made conditional on the reception of an acknowledgement of receipt.

A data message is deemed to have been dispatched when it enters an information system that is not under control of the originator or the intermediary. Determination of the moment of reception of a data message depends on whether or not the addressee has designated an information system to receive the data message.

If the addressee has designated such information system, the data message is deemed to have been received the moment it enters into the designated information system.[61] If, notwithstanding that the addressee has designated an information system, the data message is sent to a different information system of the addressee, the data message is deemed to have been received when it is actually retrieved by the addressee.[62] If no information system has been designated by the addressee, the data message is deemed to be received when:

1. It is actually retrieved by the addressee;[63] or
2. It enters an information system of the addressee.[64]

The rules mentioned above are applicable to the determination of the moment of reception of the data message, even if the relevant information system is located in a place different than the place of reception determined pursuant to the relevant provisions of law.

**Place** Unless otherwise agreed between the originator and the addressee, a data message is deemed to be:

1. Dispatched at the place where the originator has its establishment;[65] and
2. Received at the place where the addressee has its establishment.

If the originator or addressee has more than one establishment, the relevant establishment is:

1. That with the closest relationship with the underlying transaction; or
2. If there is no underlying transaction, its principal establishment.

---

61 Code of Commerce, article 91(I).

62 Code of Commerce, article 91(II).

63 Code of Commerce, article 91(II).

64 Code of Commerce, article 91(III).

65 Mexican law uses the word "establishment" (*establecimiento*) rather than "place of business", as the English version of the 1996 Model Law does. The two terms, however, are equivalent and, in fact, the Spanish version of the 1996 Model Law uses the term "establishment".

If the originator or addressee does not have an establishment, its habitual residence place will be considered.

## 16.03 Electronic Commerce in Specific Areas

### (a) Carriage of Goods

Unfortunately, and despite the fact that Title 2 is generally applicable to acts of commerce involving contracts of carriage of goods, the Mexican legislator did not incorporate the provisions of articles 16 and 17 of the 1996 Model Law, which generally provide that data messages can be used in lieu of written or other paper documents in actions related to these contracts, including issuing receipts for goods, claiming delivery, and acquiring and transferring rights and obligations under the contract.

Thus, the question arises as to whether the provisions of Title 2 also are applicable to contracts of carriage of goods. This issue will have to be finally resolved by the Mexican courts but, given the terms pursuant to which the sphere of application of Title 2 is stated (see text, above), the answer should be affirmative, even in connection with the issuance and assignment of bills of lading (*carta de porte*) that must be issued by the relevant carrier and that are negotiable instruments under Mexican law.

### (b) Consumer Contracts

The provisions of Title 2, as well as the e-commerce law provisions incorporated directly into the Federal Civil Code, also are applicable to consumer contracts, which are generally governed by the Federal Consumer Protection Act.

As part of the 2000 E-Commerce Decree, Congress added a chapter to the Federal Consumer Protection Act, entitled "Of Consumers' Rights in Transactions Carried Out by the Use of Electronic or Optical Means or Any Other Technology". The provisions of the chapter apply to all types of electronic transactions carried out between suppliers or providers of goods and services with consumers. They establish a set of principles to which suppliers must adhere in electronic transactions, and they are intended to protect consumers and the privacy of their personal data.

Suppliers must use the information provided by consumers in a confidential manner, and they may not disclose it or transfer it to other suppliers not involved in the transaction, unless the disclosure or transfer has been expressly approved by the consumer or on legal request from an authority Suppliers must use an available technical element to provide security and confidentiality for the information provided by consumers, and they must inform them, prior to the execution of the transaction, of the general features of such element.

Prior to executing the transaction, suppliers must provide the consumer with the provider's "physical" address, telephone numbers, and other means available for the consumer to submit its claims or requests for information to the supplier.

Suppliers must avoid using deceitful commercial practices regarding the characteristics of the products, for which reason they must comply with the Federal Consumer Protection Act and related provisions regarding information and advertising.

Consumers are entitled to know all the information regarding the terms, conditions, costs, surcharges, and forms of payment of the products or services offered by the supplier. Suppliers must respect consumer decisions as to whether or not the consumer wants to receive commercial advertising. In addition, other articles of the Federal Consumer Protection Act were amended to:

1. Establish, as one of the aims of the Federal Consumer Protection Act, the "effective protection of consumers in transactions executed by the use of electronic or optical means or any other technology and the adequate use of provided data"; and
2. Establish, as one of the missions of the Federal Consumer Protection Agency (*Procuraduría Federal del Consumidor*), the promotion of the issuance, publication, and use of codes of ethics by suppliers that carry out electronic transactions with consumers. The codes of ethic must incorporate the relevant principles set forth in the Federal Consumer Protection Act.

### (c) Financial Transactions

Mexican law also provides for rules applicable to the execution of electronic transactions by financial institutions, particularly banks and securities brokers. The rules are contained in several statutes applicable to banking and finance activities. In addition, these transactions are subject to many regulations issued by the financial sector's regulatory bodies.

Pursuant to the Credit Institutions Act, which regulates banks and banking, banks can agree with their users as to the execution of their operations and the provision of services by the use of "equipment, electronic, or optical means, or any other technology, automated data processing systems, and private or public telecommunications networks", provided that they establish in the relevant contract the following:

1. The agreement as to the transactions and services;
2. The means for identifying the users and the responsibilities applicable for its use; and

3. The means to be used to evidence the creation, transmission, modification, or extinction of the rights and obligations.

The use of the above-mentioned "electronic means", which are really electronic signatures, produces the same legal effects as handwritten documents, with the same evidentiary value.

These rules, contained in article 52 of the Credit Institutions Act and similar to other financial laws, were enacted prior to the 2003 E-Signatures Decree and amended on 4 June 2001. They require the execution of a pre-contract prior to the execution of electronic transactions, as the Federal Civil Code requires in the case of contracts executed by exchange of telegrams but, pursuant to the same Civil Code, the requirements are not applicable to data messages.

### (d) Taxation

The Federal Tax Code was amended in 2004 to incorporate the possibility of using some type of advanced electronic signatures and certificates for the presentation of tax returns and other tax-related activities. In fact, the Federal Tax Code mandates the use of data messages (which the Federal Tax Code refers to as "digital documents") and of advanced electronic signatures for filing tax returns and other filings in many cases.

The regulation of electronic filing in the Federal Tax Code is very exhaustive[66] and has a different focus (e.g., certificates of electronic signatures to be used by legal entities taxpayers are to be issued by the Tax Administration Service), and it represents a radical change towards electronic filing in government matters. It is significant that the regulation of the Fiscal Tax Code substantially draws from the 2001 Model Law and the 2003 E-Signatures Decree.

66 Federal Tax Code, articles 17-C to 17-J.