KINGDOM OF CAMBODIA

NATION RELIGION KING

LAW

ON

ELECTRONIC COMMERCE

ROYAL KRAM

NS/RKM/1119/017

WE

Preah Karuna Preah Bat Sâmdach Preah Bâromneath Norodom Sihamoni Saman Bhumichat Sasana Rakkhata Khattiya Khmeraratrat Putthintra Mohaksat Khemareacheana Samuhobhas Kampuchea Ekareacharath Bureanasanti Subheamagala Sirivibunla Khmera Sri Bireat

Preah Chao Krung Kampuchea Dhibodi

- Having seen the Constitution of the Kingdom of Cambodia;
- Having seen Royal Decree No. NS/ RKT/0918/925 dated 06 September 2018 on the appointment of the Royal Government of Cambodia
- Having seen Royal Kram No. NS/ RKT/0618/012 dated on 28 June 2018 promulgating the Law on the Organization and Functioning of the Council of Ministers;
- Having seen Royal Kram No. NS/ RKT/0196/16 promulgating the Law on the Establishment of the Ministry of Commerce;
- Having seen the Request of Samdech Akka Moha Sena Padei Techo Hun Sen, Prime Minister of the Kingdom of Cambodia

PROMULGATE

Law on Electronic Commerce which was enacted by the National Assembly on 8 October 2019 at its third plenary session off the sixth legislature, and entirely reviewed and approved by the Senate on its form and legal concept on 18 October 2019 at its extraordinary session of the fourth legislature, with the following content:

Chapter 1

General Provisions

Article 1: Purposes

The purposes of this law are as follows:

1. To govern electronic commerce in the Kingdom of Cambodia and with the international;
2. To create legal certainty in the civil and commercial transactions by electronic system;
3. To give confidence to the public in the usage of electronic communication.

Article 2: Goals

The goals of this law are as follows:

1. To determine the authenticity, perfection and reliability of an electronic form;
2. To promote the development of legal and business framework in order to conduct safe electronic commerce;
3. To prevent and enforce against acts which are harmful to data and information systems;
4. To eliminate obstacles which hinder electronic commerce and which created by the uncertainty of requirements of written documents and signature;
5. To facilitate electronic filing of documents with public institutions and promote an efficient delivery of services of public institutions through the use of reliable electronic records; and
6. To establish rules, regulations and standards regarding the authenticity and perfection of electronic records.

Article 3: Scope

This law shall apply to all activities, documents and civil and commercial transactions that are made via electronic system except for the activities, documents and transactions relating to:

1. Formation or enforcement of Power of Attorney;
2. Formation or execution of a testament, codicil or other matters relating to succession;
3. Any contract for sale, transfer or disposition of rights to immovable property or any interests in such property;
4. Transfer of immovable property or any interests relating to the immovable property; and
5. Any other exceptions as provided for by Sub-Decree.

Article 4: Definitions

All important terms use in this law are defined in the glossary found in the annex of this law.

Chapter 2

Validity of Electronic Communications

Article 5: Legal recognition of electronic communications

No one may refuse to recognize the validity, legal effect, admissibility or enforceability of an electronic communication solely on grounds that it is formed in electronic form or is in an electronic communication.

Article 6: In writing requirement

1. Where any provisions is required to provide an information in writing or recorded in writing, this requirement shall be deemed fulfilled if the information is made in an electronic form and can be accessed and retrieved for subsequent use.
2. Where the requirement in the provision of the paragraph (1) above applies, a legal requirement demanding any person to provide at the same time multiple copies of any information or matters to another person, the person subjected to such requirement may fulfil this requirement by only providing a single copy in electronic form.

Article 7: Signature requirements

1. Where any provision requires a signature of a person, such requirement shall be deemed fulfilled by an electronic signature if the electronic signature was created by means which:
    a. Can determine the identity of a person and indicate the approval of the person on information or record contained in the electronic communications.
    b. Can be trusted in accordance with the characteristics, the purpose and the circumstance for which the electronic communication was made or communicated.
2. Notwithstanding any provision that states a requirement for a signature or only states consequence for the absence of a signature, the provision of the paragraph (1) above shall also apply.

Article 8: Requirements to retain information in original form

A legal requirement to retain information that was not made electronic form may be fulfilled by the retention of such information in electronic form if:

1. Such electronic form is a reliable means to determine the completeness of the information; and
2. Such information is easily retrievable for subsequent use.

Article 9: Prescribed form

Where any provision requires that information be created in any prescribed form, such requirement shall be substituted by providing information in electronic form if the electronic form fulfils the following conditions:

1. Contains the same information or substantially the same information as prescribed form;
2. Is accessible, intelligible, and retrievable for subsequent use; and
3. Can be retained by the person who received the information.

Article 10: Record retention requirements

1. Where any provision requires that any specific document, record or information, such requirement shall be deemed fulfilled if the retention fulfils all conditions as follows:
   a. Information contained in such electronic communication is accessible and retrievable for subsequent use;
   b. Electronic communication is retained in original format in which it was created, sent or received, or in a format that can identify the accuracy of the information; and
   c. Such information is kept to allow any person can identify the origin and destination of such electronic communication, date and time when such electronic communication was sent or received.
2. Obligation to retain documents, records or information in accordance with paragraph (1) does not include any information for the sole purpose to send or receive messages.

Article 11: Evidentiary requirements

No provisions in relation to the application of rules of evidence may object to the admissibility of electronic communication as evidence only on the ground that:

1. The evidence is an electronic communication; or
2. The evidence is not in original form.

Article 12: Formation and validity of contracts

1. Offer, acceptance, and contract may be done in electronic means.
2. A contract in electronic form mentioned in the provision of the paragraph 1 above has validity, legal effect, and enforceability when the offer and acceptance coincide.

Article 13: Effect between parties

The originator and addressee of electronic communication shall not refuse the legal effect, validity or enforceability of theirs intent or declaration.

Article 14: Separate implementation by agreement of parties

1. By agreement, parties that participate in the generation, sending, receiving, storage or processing of electronic communication may disregard the provisions as stated in Chapter 2 of this law, except otherwise determined.
2. Notwithstanding the provisions as stated in Chapter 2, parties to the contract or transactions may:
   a. Refrain from using any electronic records, electronic communication or electronic

signature in the contract or any transaction as agreed between the parties; or

b. Set additional requirements in relation to form or authenticity of the contract or the transaction as agreed between the parties.

Chapter 3

Electronic Communications Process

Article 15: Time and place of dispatch and receipt of information in electronic communications

1. Information in an electronic communication is deemed dispatched when:
   a. The information leaves the information system that is under the control of the originator or of the party who sent it on behalf of the originator; or
   b. In case that the information is sent but it has not left the information system that is under the control of the originator or of the party who sent it on behalf of the originator, the information is deemed that it is dispatched when such information is received at any time.
2. Information in an electronic communication is deemed to be dispatched from the place of business of the originator, no matter where it is dispatched.
3. The time of receipt of an information is the time when the information becomes capable of being retrieved by the addressee at the electronic address designated by the addressee. The information is deemed to be received at the place where the addressee has its place of business.
4. If a specific electronic address has not been provided by the addressee, the time of receipt of an information is the time when the addressee becomes aware of the dispatch and retrievability at any electronic address and the information is deemed to be received at the place of business of the recipient.
5. If the electronic address is provided by the addressee, the information in the electronic communication is deemed to be received when it reaches the electronic address of the addressee, and is deemed to be received at the place where the addressee has its place of business.

Article 16: Offer for forming a contract

Any proposal to enter into a contract through an electronic communication which is not addressed to any other specific person is considered as an invitation to make an offer for forming a contract only. The proposal will be considered as an offer for creating a contract if the proposal clearly indicates the intention of the party that it shall be bound when there is an acceptance from the other party.

Article 17: Use of automated system for contract formation

A contract formed by the interaction of an automated system of a person with any natural person, or with the automated systems of another person, shall not be denied validity, legal effect, or enforceability of the contract on the ground that no natural person directly reviewed or intervened in the automated system or in forming the contract.

Article 18: Error of information input in electronic communication

Where a natural person makes an information input error in an electronic communication with the automated system of another party, and the automated system does not provide the person with an opportunity to correct the input error, that person, or the party on whose behalf that person was acting, has the right to make correction or withdraw the input error in case:

1. The person notifies the other party of the error as soon as possible after having learned of the error, and indicates that he had made an error in the electronic communication; and
2. The person has not benefitted in any way from the error, prior to notification to the other party, and has not caused any damages of interest to the other party or any third party.

The provision as stated in this Article shall not be applicable to the securities sector.

Chapter 4

Secure Electronic Records and Electronic Signatures

Article 19: Secure electronic record

An electronic record shall be considered as a secure electronic record, only if it is properly applied in accordance with the secure procedure which ensures that the electronic record has not been altered commencing from any specific point in time to the time of verification.

Article 20: Secure electronic signature

1. An electronic signature is secure only if it complies with the conditions below:
    a. Can be uniquely linked to only one signatory;
    b. Is capable of identifying the signatory;
    c. Is created by using means that is under the management of signatory;
    d. Confirm the date and time of the signature; and
    e. Confirm the original status of messages or the electronic record which is linked the signature.
2. The provision of the paragraph (1) above shall not limit the ability of any person in an electronic communication to:
    a. Establish/set additional conditions in relation to the reliability of electronic signature; or
    b. Adduce evidence of non-reliability of an electronic signature.

Article 21: Presumptions relating to secure electronic records and signatures

1. Unless there is evidence to the contrary, in any proceedings involving a secure electronic record, the secure electronic record is presumed as an electronic record which has not been altered since a specific point in time.
2. Unless there is evidence to the contrary, in any proceedings involving a secure electronic signature, a secure electronic signature is presumed as follows:
    a. The electronic signature is the signature of the related person; and
    b. The electronic signature was affixed by a person with the intention of signing or

approving the electronic record.

3. In the absence of a secure electronic record or a secure electronic signature, nothing in any provisions of the Chapter 4 shall create any presumption relating to the authenticity or accuracy of the electronic record or electronic signature.

Article 22: Use of stolen identity

All person shall not use the identity, record, electronic signature, electronic address, secret code, or feature of other persons in bad faith or without permission in a commercial or non-commercial transaction via electronic system.

Article 23: Competent institution to manage the security procedures

1. The Ministry of Posts and Telecommunications shall be the competent institution to manage security procedures for the electronic record and the electronic signature.

2. The management of the secure procedures for the electronic record and the electronic signature shall be determined by regulations.

Chapter 5

Intermediaries and Electronic Commerce Service Providers

Article 24: Liability of intermediaries and electronic commerce service providers

1. An intermediary or an electronic commerce service provider shall not be subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of service provision of the intermediary and the electronic commerce service provider, if the intermediary and electronic commerce service provider was not the sender/originator of the record and in the case that:

   a. The intermediary or electronic commerce service provider has no actual knowledge that the information gives rise to civil or criminal liability;

   b. The intermediary or electronic commerce service provider is not aware of any facts or circumstances which they ought to know reasonably give rise to a likelihood of civil or criminal liability in respect of the information; or

   c. The intermediary or electronic commerce service provider becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known and take action in accordance with the procedure set out in Article 25 in relation to unlawful information and defamation in below.

2. An intermediary or electronic commerce service provider shall not be required to monitor any electronic record processed by the electronic system which is under his management whether its processing would constitute or give rise to an offence or give rise to civil liability unless otherwise provide/determine.

3. Provision of this article shall not apply to an intermediary or electronic commerce service

provider to be free from:

a. Any obligation established pursuant to a law or legal norms /regulations;

b. Any obligation to comply with an order or direction of a court or other competent authority; or

c. Any contractual obligation.

Article 25: Liability for information or event

1. If an intermediary or an electronic commerce service provider is aware that that the information in an electronic record gives rise to civil or criminal liability, the intermediary or the electronic commerce service provider shall immediately take measure as bellow:

   a. Remove the information from any information system within the intermediary's or the electronic commerce service provider's control and cease to provide services in respect of that information;

   b. Preserve the information as evidence and notify the Ministry of Posts and Telecommunications or relevant competent institutions about the facts and the identity of the suspected person.

2. In the event that an intermediary and an electronic commerce service provider is aware of any facts or circumstances which may lead to the civil or criminal liability, the intermediary and the electronic commerce service provider shall preserve the information evidence and notify the Ministry of Posts and Telecommunications or relevant competent ministries-institutions.

3. When it is acknowledged or notified in respect of any information of electronic record which may be subject to civil or criminal liability, the Ministry of Posts and Telecommunications and relevant competent ministries-institutions may give an instruction to the intermediary or electronic commerce service provider to perform any operation as follows:

   a. Remove the electronic record from the system which is under its control;

   b. Suspend or cease to provide services to the person; or

   c. Suspend or cease to provide services in respect of that electronic record.

4. An intermediary or an electronic commerce service provider is not liable on civil liability, whether in contract, outside of contract or in accordance with the law in respect of an activity performed in good faith as directed by the Ministry of Posts and Telecommunications or relevant competent ministries-institutions.

5. Any person who lodges a notification of unlawful activity with an intermediary or an electronic commerce service provider bout illegal activity knowing that the notification is false or misleading shall be subject to civil or criminal liability in respect of such offense.

Article 26: Provision of issuance of a permission letter or a license

1. An intermediary and an electronic commerce service provider shall request for a permission letter or a license from the Ministry of Commerce and the Ministry of Posts and Telecommunications.
2. The Ministry of Commerce provides a permission letter or a license including:
   a. A permission letter to operate an electronic business for a natural person.
   b. A license to allow the operation of electronic commerce service provision for a legal person.
3. The Ministry of Posts and Telecommunications shall provide an online service certificate.
4. The exception, the determination of type for license, the formalities, and the procedure of providing a permission or license shall be determined by a sub-decree.

Article 27: Professional code of conduct and regulations on intermediaries and electronic commerce service providers

1. An intermediary or an electronic commerce service provider shall comply with the approved professional code of conduct and regulations relating to electronic commerce determined by inter-ministerial Prakas between the Ministry of Commerce and the Ministry of Posts and Telecommunications.
2. The professional code of conduct referred to the provisions in paragraph (1) shall be determined and prepared by the Ministry of Commerce and the Ministry of Posts and Telecommunications in cooperation with the relevant competent ministries-institutions and related parties.

Article 28: Tax obligation, incentives and preferences

An intermediary and an electronic commerce service provider shall be subject to the common legislation of the applicable tax regime and shall receive the incentives and preferences in accordance with the laws and regulations in force.

Chapter 6

Consumer Protection

Article 29: Minimum information in electronic commerce

1. A person using electronic communications to sell goods or services to consumer shall provide accurate, clear and intelligible information and must have at least the following information:
   a. Name or legal name of the person, the registered business address and an electronic means for contact or a telephone number;
   b. Form of prompt, easy and effective communication between consumers and the

seller;

c. Terms, conditions and costs of goods or services associated with a commercial transaction, particularly the terms and conditions, and methods of payment, and details related to withdrawal or cancellation of the purchase order, termination, return and exchange of goods, and refund; and

d. Actual goods and services offered for sale.

2. The information provided in the provisions of the paragraph (1) above shall be sufficient to enable consumers to make a decision about the commercial transaction and to retain the information.

3. The provisions of this Article shall not apply to the securities and insurance sector.

Article 30: Unsolicited communications

Any person, whether or not having a place of business inside or outside the Kingdom of Cambodia, who sends unsolicited commercial communications to consumers based in or out of the Kingdom of Cambodia through an electronic media or through an intermediary or a telecommunication service provider shall provide the consumer with a clearly specified and easily activated option to reject the unsolicited commercial communication.

Article 31: Formation of Counterfeit Electronic System and Malicious Code

1. Any person shall not create an electronic system for the purpose of counterfeiting or causing a confusion in order to take advantage, or in the purpose of attracting to have a usage or an operation, and lead to have an injury/damage to the person who used it or to the third party.

2. Any person shall not create, provide, enable, distribute, or send the virus-code in the bad-faith purpose through electronic means in to electronic instrument or system of other persons.

Article 32: Data protection

1. Any person that holds personal information in electronic form shall use all means to ensure that the information is protected by such security safeguards as it is reasonable in every circumstances to avoid the loss, access, use, modification, leak or disclosure of those information, except with the permission of the owner of the information or any other party authorized by law.

2. Any person shall not interfere in the electronic system, access, retrieve, copy, extract, leak, delete or modify data, which is under the retention of any other person in bad-faith or without permission.

Article 33: Implementation of provisions related to consumer protection

Any person using electronic communications for commercial activities with consumers shall comply with all other provisions and regulations related to consumer protection.

Chapter 7

Government Activities and Transactions via Electronic System

Article 34: Acceptance of electronic communications by state institutions

1. Ministries or institutions of the government may use the following actions and transaction in electronic form:
    a. The filing of documents or the fulfilment of requirements for document creation or retention;
    b. Issuance of any license or permission letter;
    c. Provision for the method and manner of payment; or
    d. Other authorized activities as determined by the state ministries-institutions.
2. In any case where the state ministries-institutions decides to use electronic communications in any activities or transaction as stated in the provisions of the paragraph (1) above, such ministry or institution/agency may specify:
    a. The manner and form in which such electronic communication information shall be filed, created, retained or published;
    b. The type and form of signature required when there is a requirement for a signature in the electronic communication;
    c. The manner and form in which such signature shall be affixed to the electronic communication;
    d. Control processes and procedures as appropriate to ensure accuracy, security and confidentiality of electronic communications or payments; and
    e. Any other conditions required to be equivalent as documents or electronic payment with that documents or payment in written format.

Chapter 8

Electronic Evidences

Article 35: General admissibility of electronic evidence

Nothing in the provisions of rules on any evidence shall apply to deny the general admissibility of an electronic record as evidence on the sole ground that it is an electronic record, even if the evidence is not in its original form.

Article 36: Perfection of the electronic system

1. In any legal proceeding, the validity of electronic evidence may be satisfied on proof of the perfection of the electronic system in or by which the data was recorded or stored.
2. In the absence of evidence to the contrary, the electronic system in which used for recording and storing for electronic recording is presumed perfection in any legal proceeding shall be in according with one of the following conditions:

a. Where evidence is adduced that supports a fact finding/confirming that the electronic system or other similar instrument was operating properly is when the electronic recording is presumably recorded and stored or when it is used as evidence or in the event that the electronic system or other similar instrument was not operating properly or not working at all but the perfection of the electronic record was not affected by such circumstances, and there are no other reasonable grounds to doubt the perfection of the record;

b. Where it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it as evidence in accordance with legal procedures; or

c. Where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to use/introduce the electronic record as evidence in the proceedings in accordance with legal procedures.

Article 37: Perfection of information

1. In the absence of evidence to the contrary, an electronic record made or stored in an electronic system is presumed to be proven that it has a perfection in any legal proceeding if the electronic record:

   a. Has remained complete and unaltered, apart from the addition of any endorsement; or any immaterial change which arises in the normal course of communication, storage or display;

   b. Has been certified or has been signed in an electronic format, by a method provided by a duly licensed security procedure provider;

   c. Has its perfection and content certified by competent ministries or institutions;

   d. Has been recorded in a storage device, or any other electronic means that does not allow alteration of the electronic records;

   e. Has been examined and its perfection confirmed by an expert appointed by the Court;

   f. When there is evidence supporting a fact finding/confirming that at all material times the electronic system or other similar instrument was operating properly during/at important times, or if not, that in any respect in which it was not operating properly or out of operation, the perfection of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the perfection of the record; or

   g. When there is evidence proving that the electronic record was recorded or stored by a party participating in the legal proceedings who is adverse in interest to the party seeking to use the electronic record;

2. When there is evidence proving that the electronic record was recorded or stored as usual and for the purpose of ordinary course of business by a natural person who is not a party to the legal proceedings, and such natural person did not record or store it under the control of the party seeking to use the record.

3. Where a report contained in an electronic record produced by an electronic system does not constitute hearsay, such report shall be admissible if the conditions specified in the provisions of the paragraph (2) related to the electronic record are met.

Article 38: Printouts

Any printouts with the original content from the electronic records can be used as evidence in legal proceedings.

Article 39: Burden of prove the authenticity of electronic evidence

1. The person requesting to introduce an electronic record in any legal proceeding shall be responsible for showing its authenticity with evidence to support the electronic record to be introduced.
2. In the case where there is any provisions which protects the vulnerable persons, including consumers and children, and which establishes the burden of introducing evidence that provides more benefits to those individuals than this law does, the provisions shall prevail over this Article.

Article 40: Standards of recording or preserving of electronic records

For the purpose of determining, under any other provisions, as to whether or not an electronic record is admissible, evidence may be presented based on standard, procedure, usage or practice on how an electronic record is to be recorded or preserved by taking into consideration the type of business, the nature and the purpose of the electronic record.

Article 41: Issuance of an authenticity certificate

1. Any person wishing to prove the authenticity of an electronic record as evidence, he/she can request for the evidence from the expert with respect to the authenticity of the electronic record in the form of a certificate.
2. The authenticity certificate under the provision of paragraph 1 above shall be issued by:
    a. Competent ministries - institutions or a person responsible in relation to the operation or management of a specified security procedure provider or a security procedure provider recognized by the Court; or
    b. An expert appointed or recognized by the Court.
3. A person who has the authority to issue the authenticity certificate as mentioned in the provision of paragraph 2 above shall not falsify or issue a false or unreal authenticity certificate of a record or electronic evidence.

Article 42: Other Procedures for the Production of Electronic Evidence

In addition to the means of proof referred to in this law, electronic evidence may be produced by means of alternative techniques and procedures, such as certification by a notary or competence institutions, recording on non-rewritable electronic medium, and electronic system forensics result in the course of judicial discovery.

Article 43: Violation of Coding

Any person shall not encode in electronic communications via electronic system which is an evidence that could lead to an accusation or encode the data or evidence in electronic system in relation to an offense.

Article 44: Admissibility of Electronic Records from Foreign Countries

Electronic evidence confirmed by competent ministries or institutions of foreign states shall be admissible as evidence if the perfection/integrity of the electronic system which records or stores the electronic record comply with the accuracy standards provided for in Chapter 8 of the law.

Article 45: Admissibility of Electronic Information from Foreign Countries

In order to determine as to whether or not the information in the electronic form is admissible or admissible to a certain degree, it is not necessary to determine the place where such information was produced or used or where the place of business was established overseas as long as such electronic record can accessible and retrievable in the jurisdiction of the Kingdom of Cambodia.

Chapter 9
Electronic Payments and/or Electronic Funds Transfers

Article 46: Electronic Payment Transaction

1. Any person operating a payment system, providing a payment service, issuing an electronic payment instrument or providing an electronic means of payment, or conducting any other operations to the public considered to be an electronic payment and shall obtain prior authorization or license from the National Bank of Cambodia.

2. The National Bank of Cambodia shall be the competent authority to formulate regulations relating to electronic payment.

Article 47: Responsibilities of Payment Service Providers

1. Payment service providers shall not provide the customers with an unsolicited payment instruments except in case of card expiration or replacement.

2. Before executing an electronic fund transfer, the payment service providers shall clearly identify the customers' identity and re-authenticate the electronic fund transfer. The payment service providers shall be held liable in the following cases:

    a. Execution of a transaction without authorization of the customers;

    b. Execution of a fund transfer after receiving report of forgery, loss, or theft of the electronic fund transfer instruments;

    c. Execution of a transaction despite the notification from the customers as defined in Article 48 below;

    d. Failure to comply with the instruction of the customers or an execution which is not in compliance with the customer's instruction; or

    e. Technical malfunction, an error in operating the technical system, or a flaw in the electronic fund transfer instruments.

3. The payment service providers shall not be held liable in case of force majeure event or customers' defaults.

4. In the case where the payment service providers are to be held liable, the service providers shall reimburse to the customer no later than 30 (thirty) days from the date of receiving the notification of the customer as defined in Article 48 of this law the transaction fee, charges, and a fine for late payment resulting from this transaction, without accounting for damages which may be suffered by the customer.

5. Any person shall not, without authorization, issue a card or transform the card into another form different from that of the original in bad faith for forgery or cheating purposes, which could cause damage/injury to another person.

Article 48: Responsibilities of Customers

1. Customers shall notify the payment service providers of any unauthorized, mistaken or wrongful transaction of their own account.
2. Customers shall notify the payment service providers or the establishment authorized by the payment service providers of any loss or theft of electronic transfer instrument or electronic fund transfer method or theft of data, which can be used with the payment instrument. Such notification shall be made in writing or by any electronic means which is acceptable to the payment service providers, and shall notify as soon as possible not exceeding 2 (two) days after the theft or loss of electronic transfer instrument is discovered.
3. In case where there is sufficient evidence proving that the loss or damage is caused by customer's default, the payment service provider shall have rights to demand the customer to be fully responsible for such loss or damage.
4. If there is no evidence to prove the customer's default, the payment service provider shall be fully and unconditionally responsible for such loss or damage.

Chapter 10
Competency, complaint and Procedures for a Fine

Article 49: Competency

A written warning, cease of business activities or transaction, suspension, revocation or cancellation of an authorization or license and imposition of a fine shall fall within the competency of the Ministry of Commerce and the Ministry of Posts and Telecommunications.

In case where a person refuses to comply with above measures, the Ministry of Commerce and the Ministry of Posts and Telecommunications may refer the case to the competent court.

Article 50: Procedures for a Complaint

1. Those who are not satisfied with the written warning, cease of business activities or business transaction, suspension, revocation or cancellation of the authorization or license and a fine by the Ministry of Commerce and the Ministry of Posts and Telecommunications shall be entitled to lodge their complaint with the Minister of Commerce and the Minister of Posts and Telecommunications.
2. The Minister of Commerce and the Minister of Posts and Telecommunications shall make

decision within 30 (thirty) days at the latest.

3. Any person who are not satisfied with the decision of the Minister of Commerce and the Minister of Posts and Telecommunications shall have the rights to lodge their complaint to the competent court of the Kingdom of Cambodia within 30 (thirty) days at the latest from the date of receipt of the notification of the decision.

Article 51: Procedure for Imposing a Fine

Procedure for imposing a fine, payment of a fine, management of fining receipt and disposition of the proceeds derived from such fines as prescribed in the provisions of this law shall be determined by an inter-ministerial Prakas between the Minister of Economy and Finance, the Minister of Commerce and the Minister of Posts and Telecommunications.

Chapter 11
Penalties

Article 52: Sanction

Sanctions in this law shall include a written warning, cease of business activities or business transactions, suspension, revocation or cancellation of the authorization or license, penalty, imprisonment and a (monetary) fine.

Article 53: Offence for Identity Theft

To be punishable by an imprisonment from 6 (six) months to 3 (three) years and a fine from 1,000,000 (one million) Riel to 6,000,000 (six million) Riel for those who act in violation of the provision in Article 22.

Article 54: Offence for Failure to Report of an Information or a Fact

To be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine from 100,000 (one hundred thousand) Riel to 2,000,000 (two million) Riel for the intermediary and the electronic commerce service providers who act in violation of the provisions of paragraph 1 and paragraph 2 of Article 25.

Article 55: Provision of False Information

To be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine from 100,000 (one hundred thousand) Riel to 2,000,000 (two million) Riel for those who commit act as prescribed in the provision of paragraph 5 of Article 25.

Article 56: Executing of an Unauthorized Transaction

To cease business activities or business transaction and be subjected to a monetary fine not exceeding 10,000,000 (ten million) Riel for those who act in violation of the provision of paragraph 1 of Article 26.

If any person used to be subjected to the measure prescribed in paragraph 1 already, and the same offence has been committed, he/she shall be punishable by an imprisonment from 1 (one) year to 3 (three) years and a fine from 2,000,000 (two million) Riel to 6,000,000 (six million) Riel.

Article 57: Offence for Failure to Comply with the Provision Regarding Minimum Information in Electronic Commerce

To be subjected to a written warning for those who act in violation of the provisions in paragraph 1 and paragraph 2 of Article 29.

Where the written warning was once given, but the same offence as prescribed in paragraph 1 above has been committed, the license or the authorization of the electronic commerce provider shall be suspended or revoked.

Article 58: Offence for Sending an Unsolicited Business Communication

To be subject to a written warning for those who act in violation of the provisions of Article 30.

Where the written warning was once given, but the same offence has been committed as set forth in paragraph 1 above, the licensed or authorized of an intermediary or the electronic commerce service provider shall be suspended or revoked or disable the media or closed down the electronic medium of the originator.

Article 59: Offence for Electronic System Forgery and Malicious Code

To be punishable by an imprisonment from 6 (six) months to 3 (three) years and a fine from 1,000,000 (one million) Riel to 6,000,000 (six million) Riel for those who act in violation of the provisions of Article 31.

Article 60: Offence for Failure to Comply with Data Protection Obligations

To be punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riel to 4,000,000 (four million) Riel for those who store information in an electronic form for a personal purpose, which is contrary to the provision of paragraph 1 of Article 32.

To be punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riel to 4,000,000 (four million) Riel for those who act in violation of the provision of paragraph 2 of Article 32.

Article 61: Offence for Violation of Authenticity Issuance

To be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine from 100,000 (one hundred thousand) Riel to 2,000,000 (two million) Riel for those who act in violation of the provision of paragraph 3 of Article 41.

Article 62: Offence for Coding Violation

To be punishable by an imprisonment from 1 (one) year to 3 (three) years and a fine from 2,000,000 (two million) Riel to 6,000,000 (six million) Riel for those who act in violation of the provision of Article 43.

Article 63: Offence for an Electronic Payment Transaction

To be punishable by an imprisonment from 1 (one) year to 5 (five) years and a fine from 1,000,000 (one million) Riel to 10,000,000 (ten million) Riel for those who act in violation of the provision of paragraph 1 of Article 46.

Article 64: Offence for Electronic Payment Instrument Forgery

To be punishable by an imprisonment from 1 (one) year to 3 (three) years and a fine from 2,000,000 (two million) Riel to 6,000,000 (six million) Riel for those who act in violation of the provision of paragraph 5 of Article 47.

Article 65: Criminal Responsibility of a Legal Entity

1. A legal entity may be pronounced to be criminally responsible in accordance with the conditions prescribed in Article 42 (criminal responsibility of a legal entity) of the Criminal Codes for offences set forth in Article 53 to Article 54, paragraph 2 of Article 56, and Article 59 to Article 64 of this law.
2. A legal entity shall be fined twice as much, plus one or more additional penalties as follows:

    a. Dissolution in accordance with the formalities determined in Article 170 (Dissolution and Liquidation of a Legal Entity) of the Criminal Code.

    b. Placement under the court surveillance according to the modalities determined by Article 171 (Placement under the Court Surveillance) of the Criminal Code.

    c. Prohibition from conducting one or more activities according to the modalities determined by Article 172 (Prohibition from Operating Activities) of the Criminal Code;

    d. Posting the decision on punishment in accordance with the formalities determined by Article 180 (Posting of a Decision) of the Criminal Code;

    e. Publication of the decision on punishment on newspapers or broadcasting on all means of audio-visual communications according to the modalities prescribed in Article 181 (Broadcasting the Decision by all Means of Audi-Visual Communications) of the Criminal Code.

Chapter 12
Final Provision

Article 66: Abrogation
All provisions contrary to this Law shall be abrogated.

Article 67: Application of this law
Once in force, this law shall be applied after 6 (six) months publication or dissemination.

PRL. 1911.1654

Saturday, 6th day of the waxing,
Month of katdeuk, Year of Pig, B.E. 2563
Done at the Royal Palace, 2 November 2019

NORODOM SIHAMNI

Having made the request to His Majesty the King
For Signature
Prime Minister

Samdech Akka Moha Sena Padei Techo HUN SEN

Having informed Samdech Akka Moha Sena Padei Techo
Prime Minister
Minister of Commerce

PAN SORASAK

Annex
Definition

The key terms used in this law shall be defined as follows:

1. **"Access"** means accessing into a computer program, a computer system, a system or an electronic network in order to communicate, transmit, store, or download data, information, or other documents contained in the electronic system by any means.
2. **"Addressee"** means a person who is intended by the originator to receive an electronic communication except an intermediary with respect to the electronic communication.
3. **"Automated system"** means a computer program, computer system, electronic system or network or other electronic means, which are used to notify or responded automatically without an intervention of any natural person.
4. **"Card"** means a card/bank card, credit/debit card, smart card, card/payment card, although in an electronic form, which bears the value and has the function for making payment.
5. **"Contaminant"** means electronic programs which are designed to:
    (a) Modify, destroy, record, transmit data or programs contained in an electronic system; or
    (b) Interfere by any means in the normal operation of an electronic system or electronic network;
6. **"Cardholder"** means the person who has named on the card and receive benefit from such a card.
7. **"Communication"** means any statement, declaration, demand, notice, request, offer or acceptance that the parties are required to make or choose to make in connection with the formation or performance of a contract.
8. **"Counterfeit card"** means any cards/payment cards which is made by fictitious, altered and false representation, depiction, or cards/payment cards which is comprised of any component of the card that is illegal.
9. **"Data"** refers to a group of numbers, characters, symbols, message, images, sound, video, information or electronic program which are prepared in a form suitable for use in database or an electronic system.
10. **"Electronic"** refers to technology having electrical, digital, magnetic, optical, biometric, electrochemical, wireless, electromagnetic, or other technologies of similar functions.
11. **"Electronic Address"** means any number or addressee which is used for sending or receiving notifications, documents, information or electronic communication.
12. **"Authenticity"** refers to an accuracy and credibility of electronic communications.
13. **"Electronic commerce"** refers to activities involving purchase, sale, rental, exchange of goods or services, including business activities and civil as well as activities and various transactions by the state through electronic system.
14. **"Electronic Payment Instrument"** means any cards/payment cards or any payment instruments which is in an electronic form and has function to make a cash payment.

15. **"Electronic communication"** means information which is communicated, processed, recorded, displayed, created, stored, received or transmitted by electronic means.
16. **"Electronic device"** means any devices designed to manage, control, and operate through electronic system.
17. **"Electronic evidence"** means any information, data or documents which are created, stored, sent or received in electronic format or electronic communication for being used to prove facts in legal proceedings, and such information, data or documents shall be authentic in accordance with the e-Commerce Law.
18. **"Electronic form"** refers to form of information, data or document which are created, sent/transmitted, received or stored in electronic system.
19. **"Electronic fund transfer"** means any transaction which is conducted through an electronic fund transfer counter or via any movable electronic devices or via electronic devices of similar functions in order to instruct banking and financial institutions to debit or credit an account.
20. **"Electronic record"** refers to a record which is made, communicated, received, stored or processed in an electronic system or which is for transmission from one electronic system to another.
21. **"Electronic commerce service provider"** means a person who uses electronic means to supply goods and/or services except for insurance establishments.
22. **"Electronic signature"** means any signatures which are created through electronic means for using to identify the signatory, including digital signature, biometric signature and other signatures.
23. **"Electronic system"** refers to an electronic device or a group of devices interconnected or inter-related via an electronic program, which may perform automatic processing of data, information or documents, including electronic devices for the storage of such data, information or documents.
24. **"Information system"** refers to a system for generating, sending, receiving, storing or otherwise processing electronic records.
25. **"Intermediary"** refers to a person who providing services, sending, receiving, transmitting or storing services, either on a temporary or permanent basis, of the electronic communication or provides other services relating to the electronic communication, including the following persons:
    1. A person representing the sender, receiver, transmitter, or the custodian;
    2. Telecommunication service providers;
    3. Network service providers;
    4. Internet service providers;
    5. Search engines providers;
    6. Online payment service providers;
    7. Online auction service providers;
    8. Online marketplaces service providers and internet commerce service provider.

26. **"Issuer"** refers to banking and financial institutions or any person who obtained approval to issues a payment card.

27. **"Malicious code"** refers to a program or a hidden function of a program that infects data, information or documents by or without leaving any trace/mark of the virus in the infected electronic file, and the virus is capable of spreading over the system with or without human intervention.

28. **"Originator"** refers to a party or a representative who initiates the operation to create, store or transmit data via electronic means, excluding the intermediary.

29. **"Payment Service Provider"** refers to banking and financial institutions or any other person who is authorized by or obtained the license from the National Bank of Cambodia to operate the payment system, issue electronic payment instrument or electronic means of payment or to conduct any operations considered to be an electronic payment to the public.

30. **"Place of business"** refers to:

    (a) A place indicated by the sender or addressee, unless there is a party who claims otherwise that the sender or addressee does not have the place of business in the area where they claim to be.

    (b) If any party has not specifically indicated his place of business, and such party has more than one place of business, the place of business shall be then the one which has the closest relationship with the contract involved, taking into consideration the circumstances known to or examined by the party any time before or during the time of executing the contract.

    (c) For a natural person who has no place of business, the place of business shall be their permanent address.

    The followings shall not be a place of business of a party:

    - A place where the technology materials or equipment of the information system are used;
    - Electronic address or domain name which is attached to the location of a party.

31. **"Record"** refers to information, data or documents which is recorded, stored or otherwise inserted in a tangible form or stored in an electronic, paper-based or other forms and is retrievable in visible form.

32. **"Service provider"** refers to:

    (a) A person who provides an information and communication services including sending, receiving, storing or processing the electronic communication or providing of services through other electronic systems;

    (b) A person who owns, possesses, operates, manages or controls a public switched network or a person who provides telecommunication services; or

    (c) Any other person who processes or stores data for the use of electronic telecommunication service-oriented or users of such service.

33. **"Security procedure provider"** refers to a person who develops or provides the security procedures.

34. **"Security procedure"** refers to a procedure which is established by law or a contract or a decision of any party, and is applied for the purpose of:

    (a) Verifying that the signature, communication or transaction in the electronic system is belong to particular person, or

    (b) Detecting error or alteration in the communication, or in the place where the electronic record is stored from any specific period of time.

The above security procedure may require the use of algorithms formula or codes, identifying words or numbers, coding, answerback (secret question) or acknowledgment of any procedures, or similar security devices.

35. **"Writing/written"** refers to any information or other records which is written, inscribed or printed on paper or other materials.

36. **"Email or Electronic Message"** refers to message or information which is created or sent or received from electronic system, indulging attachments in texts, image, sound, video, and any electronic record which can be transmitted with the message.

37. **"Succession"** or **"Will"** refers to the assignment of right and duties of the decedent to one or more successors at will or by law.

38. **"Acceptance"** refers to an expression of will in which a person has expressed his consent to an offer made by other persons in order to form a contract.