

## **Chapter 1 General Provision**

### **Article 1- Purpose**

This law establishes criminal provisions to enhance the effectiveness of combatting online scams, with the aim of preserving and protecting security and public social order, and strengthening cooperation in combating these crimes.

### **Article 2- Scope**

This law applies to fraud committed through technological system or by using technology as a means to commit the offense, as well as to other offenses related to such activities.

The offense covered by this law include those under any of the following circumstances:

- 1- The offense is committed or deemed to have been committed within the territory of the Kingdom of Cambodia, in accordance with the provisions of the Criminal Code in force.
- 2- The offense is committed outside the territory of the Kingdom of Cambodia in any of the following cases:
  - The offense is committed by a Cambodian national;
  - The offense is committed against a Cambodian national;
  - The property suspected of being related to the offense, or the proceeds of such offense as stipulated in this law, which has been transferred into or out of the Kingdom of Cambodia;
- 3- The offense is committed through the use of the banking or financial system of the Kingdom of Cambodia.

## **Chapter 2 Competent Authority**

### **Article 3- Mechanism for Combating Online Scams**

Combatting against online scams is the responsibility of the judicial police officers and shall be carried out in accordance with the provisions of the Code of Criminal Procedure. When necessary, the Royal Government may establish a separate mechanism for combating online scams to lead, coordinate, supervise and implement efforts to prevent, suppress and combat online scams, as well as other crimes stipulated in this law, and to promote international cooperation in combating such crime.

The coordination of responsibilities between the judicial police officers and this mechanism shall be determined by the Royal Government.

#### **Article 4- Accreditation as Judicial Police Officers**

Civil servants who are responsible for combating against online scams within the mechanism established under Article 3 (Mechanism for Combating Online Scams) of this law are accredited as judicial police officers for the purpose of examining, investigating, and inquiring into online scams and other crimes stipulated herein, in accordance with the Code of Criminal Procedure. The accreditation of civil servants working within this mechanism as judicial police officers shall be granted by Prakas of the Minister of Justice.

The oath-taking and performance of duties of judicial police officers shall be conducted in accordance with Code of Criminal Procedure.

### **Chapter 3 Offenses Related to Online Scams**

#### **Article 5- Online Scams**

Online scams are acts of deceiving a natural person or legal entity by the use of dishonest maneuvers, committed through technological systems or by using technological systems as a means, with the aim of obtaining:

- 1- The transfer of funds, valuables or any property;
- 2- The provision of service;
- 3- The making of document that incur or discharge an obligation.

Online scams shall be punishable by imprisonment from 2 (two) years to 5 (five) years and a fine from 200,000,000 (two hundred million) Riels to 500,000,000 (five hundred million) Riels.

Online scams shall be punishable by imprisonment from 5 (five) years to 10 (ten) years and a fine from 500,000,000 (five hundred million) Riels to 1,000,000,000 (one billion) Riels when the act is committed:

- 1- By organized criminal group; or
- 2- Against multiple victims.

#### **Article 6- Organizing or Directing an Online Scams Center**

The act of organizing or directing a place for committing online scams through technological systems, which is centralized or structured in the form of a centre which allows multiple individuals to assemble as a group or network, whether with or without a defined management structure, for the purpose of committing online scams, shall constitute the offense of organizing or directing an online scams center. Such offense shall be punishable by imprisonment from 5 (five) years to 10 (ten) years and a fine from 500,000,000 (five hundred million) Riels to 1,000,000,000 (one billion) Riels.

It shall be deemed to constitute the offense of organizing or directing an online scams center and shall be subject to the penalties prescribed in paragraph 1 above for the act of organizing or directing separate places, but are connected or coordinated as a network in any form to commit online scams, even if not centralized in the form of a center.

The act of organizing or directing an online scams center shall be punishable by imprisonment from 10 (ten) years to 20 (twenty) years and a fine from 1,000,000,000 (one billion) Riels to 2,000,000,000 (two billion) Riels when the act is committed:

- 1- By using violence, torture, or act of cruelty;
- 2- By arrest, detention, or confinement;
- 3- By migrant smuggling, human trafficking, labor exploitation, coercion to act against one's will or other forms of exploitation.

Where the act of organizing or directing an online scams center results in the death of one or more persons, it shall be punishable by imprisonment from 15 (fifteen) years to 30 (thirty) years or by life imprisonment.

#### **Article 7- Recruiting or Training Others to Commit Online Scams**

The act of recruiting or training others for the purpose of committing online scams shall be punishable by imprisonment from 2 (two) years to 5 (five) years and a fine from 200,000,000 (two hundred million) riels to 500,000,000 (five hundred million) riels.

The act of recruiting or training others to commit online scams shall be punishable by imprisonment from 5 (five) years to 10 (ten) years and a fine from 500,000,000 (five hundred million) riels to 1,000,000,000 (one billion) riels when the act is committed:

- 1- By the use of violence, torture or act of cruelty;
- 2- By capture, detention or confinement;
- 3- Resulting in the death of a person;
- 4- With knowledge that the person recruited or trained is a victim of migrant smuggling or human trafficking.

#### **Article 8- Collecting Identification Documents or Personal Information Documents of Others with Malicious Intent**

Any person who collects identity cards, passports, or personal information documents of others for the purpose of using or creating, including but not limited to bank accounts, online accounts, websites, electronic accounts, or social media accounts as a means of committing online scams shall be punishable by imprisonment from 1 (one) year to 3 (three) years and a fine ranging from 100,000,000 (one hundred million) Riels to 300,000,000 (three hundred million) Riels.

Where the act of collecting identification documents or personal information with malicious intent is committed by an organized criminal group, it shall be punishable by imprisonment from 3 (three) years to 5 (five) years and a fine from 300,000,000 (three hundred million) Riels to 500,000,000 (five hundred million) Riels.

**Article 9- Money Laundering Related to Offenses under the Present Law**

Where a property owner is unable to provide evidence of the lawful origin of the property suspected to be involved in the offenses of online scams or proceeds of such offenses or other related offenses stipulated in this law shall be considered a form of money laundering and shall be punishable as the offense of money laundering.

**Article 10- Additional Penalties**

The court may impose one or more additional penalties as stipulated in Article 53 (Types of Additional Penalties) of the Criminal Code for any person who commits an offense as stipulated in Articles 5 (Online Scams) to Article 8 (Collecting Identification Documents or Personal Information Documents of others with Malicious Intent) of this Law.

The court may order the confiscation, as state property, of real estate used as a location or center for online scams.

The court may also order the closure or removal of bank accounts, online accounts, websites, electronic accounts or social media accounts that were created using the identity card or passport or personal information documents of others and were used as a means of committing online scams..

The content, formality and procedures for the implementation of these additional penalties shall comply with the provisions of the Criminal Code.

**Article 11- Criminal Liability of Legal Entities**

A legal entity may be held criminally liable under the conditions set forth in Article 42 (Criminal Liability of Legal Entities) of the Criminal Code for the offenses set forth in Articles 5 (Online Scams) to Article 9 (Money laundering Offense Related to Offenses Stipulated under the Present Law) of this Law.

A legal entity shall be punishable by a fine from 1,000,000,000 (one billion) Riels to 30,000,000,000 (thirty billion) Riels or up to the value of the funds or property that are proceeds of crimes and also be subject to one or more of the additional penalties as provided in Article 168 (Additional Penalties Applicable to Legal Entities) of the Criminal Code.

**Article 12 -Attempt**

An attempt to commit a misdemeanor as stipulated in this law shall be punishable in the same way as a committed misdemeanor.

**Article 13- Criminal Liability of Accomplices, Instigators, and Co-conspirators**

Any accomplice, instigator, or co-conspirator to an offense provided for under this Law shall be punishable in the same manner as the principal offender.

**Article 14- Pronouncement of Principal Penalties**

The provisions of Article 97 (Pronouncement of Principal Penalties) of the Criminal Code shall not apply to the offenses stipulated in this law. Pronouncement of principal penalties shall be carried out in accordance with the provisions of this law.

The principal penalties for any offense as stipulated in this law may not be replaced by alternative penalties or additional penalties set forth under conditions in the Criminal Code.

**Article 15- Non-Criminal Liability of Persons Forced to Commit Online Scams**

A person who participated in the commission of an offense under the influence of a compelling force or coercion shall not be criminally liable for the offenses stipulated in this Law, in accordance with the provisions of the Criminal Code in force.

**Article 16- Exemption from Punishment and Mitigating Circumstances**

A person who participated in the commission of any offense as stipulated in Article 6 (Organizing or Directing An Online Scams Center) and Article 7 (Recruiting or Training others to Commit Online Scams) of this Law shall be exempted from punishment if, before being prosecuted, that person disclosed the existence of the criminal act to the competent authorities and such disclosure leads to the identification of other participants or to the recovery of the proceeds of crime.

However, where such disclosure is made after indictment, the person shall be entitled to mitigating circumstances. The effect of such mitigating circumstances shall be applied in accordance with the Criminal Code.

**Chapter 4**

**Provisions on Criminal Procedures**

**Article 17- Implementation Procedures**

Unless otherwise provided for in this Law, the procedures for examination, investigation, prosecution, judicial investigation, and conviction of online scams and related offenses as stipulated in this law shall be conducted in accordance with the Code of Criminal Procedure.

**Article 18- Police Custody**

Police custody shall be implemented in accordance with the Code of Criminal Procedure. Where necessary for the purpose of proceeding, the duration of police custody may be extended in

increments of 48 (forty-eight) hours with the prior authorization of the prosecutor in the following circumstances:

- The offense is committed by an organized criminal group or involves multiple suspects;
- The offense resulted in a multiple victims.

The aggregated duration of police custody shall not exceed 10 (ten) days.

Any extension of police custody shall be an exceptional measure. Each extension shall be authorized by the Prosecutor, who shall meticulously verify the factual grounds and the necessity for such extension. The judicial police officer shall record the prosecutor's authorization for extension in the formal record of police custody.

#### **Article 19- Suspension, Seizure, and Freezing**

Upon detection of suspicious transactions, or in order to prevent the transfer of funds from an account suspected of being related to an offense or the proceeds of crime under this Law, judicial police officer may directly request the Cambodia Financial Intelligence Unit to temporarily suspend the suspicious transactions. The Cambodia Financial Intelligence Unit shall suspend the transactions upon such requests promptly and without delay. The duration of suspension of suspicious transactions shall not exceed 48 (forty-eight) hours. The judicial police officer may request the prosecutor for the seizure of accounts or to the court for a freezing order of the accounts. The court may order the seizure or freezing of such accounts on its own initiative.

Upon detecting properties or suspicious transactions related to the offenses or the proceeds of crime under this Law, judicial police officer may request competent authorities to temporarily seize the property or suspend the transactions. The competent authorities shall take immediate action to temporarily seize the property or suspend the transactions.

The court shall rule on the seizure or freezing within 48 (forty-eight) hours of receipt of a request or complaint. In complex cases, an extension may be granted not exceeding 24 (twenty-four) hours.

Account holders, property owners, or affected third parties may appeal the court's decision as stated in the above paragraph after receiving notification of the interim measures, in accordance with the prevailing criminal procedures.

#### **Article 20- Professional Confidentiality**

Professional confidentiality shall not prevent the implementation of this law.

#### **Article 21- International Cooperation**

Cooperation with foreign states regarding extradition and mutual legal assistance — including but not limited to inquiry, investigation, and suppression of crimes, as well as information collection

and exchange, identification of suspects, assets tracing, seizure and freezing of property, and the recovery of proceeds of crime related to online scams shall be carried out in accordance with the laws of the Kingdom of Cambodia and international instruments concerning combating transnational crimes and cybercrimes to which Cambodia is a party.

#### **Article 22- Confiscation of Property**

Where charges are dismissed because the perpetrator remains unidentified or has deceased, the investigating judge may submit order to the criminal court to decide on the confiscation of instruments, materials, funds, proceeds, or property used as means in the commission of the crime, crime site, or proceeds of the crime as stipulated in this law, in accordance with the Code of Criminal Procedure.

#### **Article 23- Application of the Law on Anti-Money Laundering and Combating the Financing of Terrorism**

In addition to the provisions herein, all provisions set forth in the Law on Anti-Money Laundering and Combating the Financing of Terrorism shall apply to anti-money laundering measures related to the offenses set forth in this law.

### **Chapter 5**

#### **Final Provision**

#### **Article 24- Promulgation and Enforcement**

The present law shall be promulgated as urgent.

The present law shall enter into force immediately.