ROYAL KRAM

WE,

នស/រកម/0426/006

HIS MAJESTY PREAH BAT SAMDECH PREAH BOROMNEATH NORODOM SIHAMONI The Loyal United Homeland, Religion, and the Protector of the Khmer Nation and its People; Sovereign of the Khmer Kingdom; Great King of the Buddhist Realm; High Provider of Security, Independence, Sovereignty, Peace, Happiness, and Prosperity for the Khmer Land and its Illustrious People; King of the Kingdom of Cambodia.

- Having seen the Constitution of the Kingdom of Cambodia;
- Having seen Royal Decree No. នស/រកត/0823/1981, dated August 22, 2023, on the Appointment of the Royal Government of the Kingdom of Cambodia;
- Having seen Royal Decree No. នស/រកត/0224/205, dated February 21, 2024, on the Additional Appointment of the Composition of the Royal Government of the Kingdom of Cambodia;
- Having seen Royal Decree No. នស/រកត/0924/1169, dated September 20, 2024, on the Adjustment and Appointment of the Composition of the Royal Government of the Kingdom of Cambodia;
- Having seen Royal Decree No. នស/រកត/1124/1477, dated November 20, 2024, on the Adjustment and Additional Appointment of the Composition of the Royal Government of the Kingdom of Cambodia;
- Having seen Royal Kram No. នស/រកម/0618/012, dated June 28, 2018, promulgating the Law on the Organization and Functioning of the Council of Ministers;
- Having seen Royal Kram No. នស/រកម/0196/04, dated January 24, 1996, promulgating the Law on the Establishment of the Ministry of Justice;
- Having seen the request of Samdech Moha Borvor Thipadei HUN MANET, Prime Minister of the Kingdom of Cambodia;

PROMULGATE

The **Law on Anti-Cyber Scam**, which was adopted by the National Assembly on March 30, 2026, during the 5th session of the 7th legislature, and reviewed entirely as to its form and legal substance by the Senate on April 3, 2026, during the extraordinary session of the 5th legislature, having the full text as follows:

Law on Anti-Cyber Scam

Chapter 1

General Provisions

Article 1: Purpose

This Law defines criminal rules to enhance the effectiveness of combatting cyber fraud, aiming to contribute to the protection of security and public order, as well as to promote the efficiency of cooperation in fighting this crime.

Article 2: Scope

This Law shall apply to fraud offenses committed through technology systems or using technology systems as a means to commit offenses, as well as offenses related to cyber fraud. Offenses falling under the scope of this Law are those committed in any of the following cases:

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 Penal 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 citizen.
    - The offense is committed against a Cambodian citizen.
    - Property suspected of being involved in the offense or the proceeds of the offense as provided in this Law have been transferred into or out of the Kingdom of Cambodia.
3. The offense is committed using the banking or financial system of the Kingdom of Cambodia.

Chapter 2

Competent Authorities

Article 3: Mechanism for Combatting Cyber Fraud Offenses

Combatting cyber fraud offenses is the competence of Judicial Police Officers, to be exercised in accordance with the provisions of the Code of Criminal Procedure. In case of necessity, the Royal Government may establish a separate mechanism for combatting cyber fraud to lead, coordinate, monitor, and implement the work of prevention, suppression, and combatting cyber fraud and other offenses provided in this Law, as well as to promote international cooperation related to fighting this crime. The coordination of competence between Judicial Police Officers and this mechanism shall be determined by the Royal Government.

Article 4: Granting of Judicial Police Officer Qualification

Civil servants in charge of suppressing cyber fraud offenses working within the mechanism established under Article 3 (Mechanism for Combatting Cyber Fraud Offenses) of this Law, shall be granted qualification as Judicial Police Officers to examine, investigate, and research cyber fraud offenses and other offenses provided in this Law, in accordance with the Code of Criminal Procedure. The granting of Judicial Police Officer qualification to the civil servants working in this mechanism shall be made by a Proclamation (Prakas) of the Minister of Justice. The swearing-in and the performance of duties of Judicial Police Officers shall be carried out in accordance with the Code of Criminal Procedure.

Chapter 3

Offenses Related to Cyber Fraud

Article 5: Cyber Fraud

Cyber fraud is an act of deceiving any natural person or legal entity by using dishonest maneuvers committed through a technology system or by using a technology system as a means, with the purpose of obtaining:

1. The delivery of funds, values, or any property.
2. The supply of services.
3. The execution of a document having the value of an obligation or a discharge. Cyber fraud 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. Cyber fraud 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 if the act is committed:
4. By an organized group.
5. Against multiple victims.

Article 6: Organizing or Leading a Cyber Fraud Center

The act of organizing or leading a place for cyber fraud characterized by a concentration of activities or in the form of a center, which allows multiple individuals to form groups or networks whether or not there is a hidden management structure to commit cyber fraud, shall be defined as the offense of Organizing or Leading a Cyber Fraud Center. This 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.

The act of organizing or leading separate locations to commit cyber fraud, which are interconnected as a network in any form, even without a concentrated center, shall also be

considered as the offense of Organizing or Leading a Cyber Fraud Center and shall be subject to the same penalties as stipulated in the first paragraph above.

The offense of Organizing or Leading a Cyber Fraud 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 if the act is committed:

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

The offense of Organizing or Leading a Cyber Fraud Center shall be punishable by imprisonment from 15 (fifteen) years to 30 (thirty) years or life imprisonment if the act causes the death of one or more persons.

Article 7: Recruitment or Training of Others to Participate in Cyber Fraud

The act of recruiting or training others with the intent to have them participate in committing cyber fraud 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 participate in committing cyber fraud 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 if the act is committed:

1. By using violence, torture, or cruel acts.
2. Through arrest, detention, or confinement.
3. By causing the death of a person.
4. With the knowledge that the recruited or trained person is a victim of human smuggling or human trafficking.

Article 8: Collection of Identification Documents or Personal Information of Others with Dishonest Intent

Any individual who collects ID cards, passports, or other personal information documents of others for the purpose of using or creating bank accounts, online accounts, websites, electronic accounts, or social media accounts as a means to commit cyber fraud, shall be punishable by imprisonment from 1 (one) year to 3 (three) years and a fine from 100,000,000 (one hundred million) Riels to 300,000,000 (three hundred million) Riels.

The act of collecting identification documents or personal information documents of others with dishonest intent 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, if the act is committed by an organized group.

Article 9: Money Laundering Related to Offenses Provided in this Law

It shall be considered a form of money laundering offense and shall be subject to the same penalties as money laundering offenses in cases where the property owner has no evidence to show the legal source of property suspected of being involved in or being the proceeds of cyber fraud or other related offenses provided in this Law.

Article 10: Additional Penalties

For any person who commits the offenses as provided from Article 5 (Cyber Fraud) to Article 8 (Collection of Identification Documents or Personal Information of Others with Dishonest Intent) of this Law, the court may declare one or more additional penalties as provided in Article 53 (Types of Additional Penalties) of the Penal Code. The court may declare the confiscation as state property of any real estate used as a location or cyber fraud center. The court may decide to close or delete bank accounts, online accounts, websites, electronic accounts, or social media accounts used as means to commit cyber fraud and which were created using the identification cards, passports, or personal information documents of others. The substance, forms, and procedures for implementing these additional penalties shall comply with the provisions of the Criminal Code.

Article 11: Criminal Liability of Legal Entities

Legal entities may be declared criminally responsible under the conditions provided in Article 42 (Criminal Liability of Legal Entities) of the Criminal Code for offenses provided from Article 5 (Cyber Fraud) to Article 9 (Money Laundering Related to Offenses Provided in this Law) of this Law. Legal entities 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 equivalent value of the funds or property that are proceeds of the offense, along with one or more additional penalties as provided in Article 168 (Additional Penalties Applicable to Legal Entities) of the Criminal Code.

Article 12: Attempt

The attempt to commit any misdemeanor provided in this Law shall be punishable the same as the completed misdemeanor.

Article 13: Criminal Liability of Principals, Instigators, and Accomplices

Principals, instigators, and accomplices of the offenses provided in this Law shall be punishable in the same manner as the perpetrators.

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 provided in this Law. The pronouncement of principal penalties shall be carried out in accordance with the provisions of this Law. Principal penalties for all offenses provided in this Law may not be substituted by alternative penalties or additional penalties under conditions as provided in the Criminal Code.

Article 15: Non-Criminal Liability of Persons Coerced to Commit Cyber Fraud

Any person who participates in committing an offense under the influence of force or coercion shall not be held criminally liable for the offenses provided in this Law, in accordance with the provisions of the Criminal Code in force.

Article 16: Exemption from Punishment and Mitigating Circumstances

Any individual who participated in committing any offense as provided in Article 6 (Organizing or Leading a Cyber Fraud Center) and Article 7 (Recruitment or Training of Others to Participate in Cyber Fraud) of this Law shall be exempted from punishment if, prior to prosecution, that person has informed the competent authorities of the existence of such acts and has led to the identification of other participants or enabled the recovery of the proceeds of the offense. However, such an individual shall receive mitigating circumstances if the aforementioned disclosure to the competent authorities is made after prosecution. The effect of these mitigating circumstances shall be implemented in accordance with the Criminal Code.

Chapter 4

Provisions on Criminal Procedures

Article 17: Implementation Procedures

The procedures for the examination, investigation, prosecution, inquiry, and sentencing regarding cyber fraud and other related offenses as provided in this Law shall follow the procedures set forth in the Code of Criminal Procedure, unless otherwise provided in this Law.

Article 18: Detention

Detention shall be carried out in accordance with the Code of Criminal Procedure. Based on the necessary requirements of the procedural implementation, the duration of detention may be extended every 48 (forty-eight) hours with the authorization of the Prosecutor in the following cases:

- The offense is committed by an organized group or involves multiple suspects.
- The offense is committed against multiple victims.

The total duration of detention shall not exceed 10 (ten) days. The extension of detention is a special measure. Every extension of detention must receive authorization from the Prosecutor, who must clearly verify the grounds and refer to the necessary requirements for the procedural implementation. Judicial Police Officers shall record the Prosecutor's decision authorizing the extension of detention in the detention report (minutes).

Article 19: Suspension, Withholding, and Freezing

In case suspicious transactions are identified, or to prevent the transfer of cash from accounts suspected of being involved in the offense or being the proceeds of the offense as defined in this Law, Judicial Police Officers may request directly to the Cambodia Financial Intelligence Unit (CAFIU) to temporarily suspend the suspicious transactions. The Cambodia Financial Intelligence Unit shall suspend such transactions immediately without delay. The suspension of suspicious transactions shall not exceed 48 (forty-eight) hours. Judicial Police Officers may request the Prosecutor to decide on withholding the account or request the Court to decide on freezing that account. The Court may decide on withholding and freezing the account on its own motion.

In case other properties or suspicious transactions are found to be involved in the offense or the proceeds of the offense as defined in this Law, Judicial Police Officers may request the competent authorities to withhold the properties or temporarily suspend those transactions. The competent authorities shall take immediate measures to withhold the properties or temporarily suspend those transactions.

The Court shall decide on the withholding or freezing of the account or property within a period not exceeding 48 (forty-eight) hours from the date of receiving the request or complaint. This period may be extended for no more than 24 (twenty-four) hours for complex offenses.

The account owner, property owner, or interested third parties may appeal against the Court's decision as defined in the above paragraph after receiving notification of this provisional measure, in accordance with the Criminal Procedure in force.

Article 20: Professional Secrecy

Professional secrecy shall not be an obstacle to the implementation of this Law.

Article 21: International Cooperation

Cooperation with foreign states regarding extradition and mutual legal assistance including but not limited to research, investigation, and suppression of offenses, as well as information collection and sharing, identification of individuals, identification of property, withholding or freezing of property, and recovery of proceeds of offenses related to cyber fraud shall be implemented in accordance with the laws of the Kingdom of Cambodia and relevant international instruments on combatting transnational crime and cybercrime to which Cambodia is a party.

Article 22: Confiscation of Property

In cases where a prosecution is dropped because the identity of the accused is unknown or the accused has deceased, the Investigating Judge may request, through a forwarding order to the criminal court, to decide on the confiscation of instruments, materials, funds, proceeds, or property used as means to commit the offense, the location of the offense, or the proceeds of the offense as defined in this Law, in accordance with the Code of Criminal Procedure.

Article 23: Implementation of the Law on Anti-Money Laundering and Combatting the Financing of Terrorism

In addition to the provisions set forth in this Law, the provisions of the Law on Anti-Money Laundering and Combatting the Financing of Terrorism shall also be applicable to anti-money laundering measures related to the offenses defined in this Law.

Chapter 5

Final Provisions

Article 24: Promulgation and Implementation

This Law is declared as urgent. This Law shall enter into force immediately.

Phnom Penh, April 06, 2026