Anti-Online Fraud Bill

Unofficial translation – May 2026

The Union Parliament has enacted this law.

Chapter (1) Name and Jurisdiction

1. This law may be called the Anti-Online Fraud Law.
2. Any of the following offences related to online fraud under this law must have jurisdiction:
    a. Offence committed within the State
    b. Offences committed on board any vessel or aircraft registered under the existing law of the State
    c. Any offence committed abroad by a person permanently residing in the country and holding an alien registration card, or by a foreigner who has been granted permanent residence in the country
    d. Offences committed within the national cyberspace or in any other cyberspace connected to the national cyberspace
    e. Offence committed by a Myanmar citizen living abroad.

Chapter (2) Description of meaning

3. The following expressions in this law shall have the meanings indicated:
    a. The State means the Republic of the Union of Myanmar.
    b. Central Committee means the Central Committee for Supervision of Combating Online Fraud established by the Union Government under this Law.
    c. Regional Committee means the Regional, State, Union Territory Online Fraud Prevention Committee formed by the Central Committee.
    d. Central Department means the Anti-Scam Centre established by the Central Committee.
    e. Ministry means the Ministry of Home Affairs which implements the matters under this law.

f. Central Bank means the Central Bank of Myanmar.

g. Online Scam means the act of deceiving someone out of money or valuables through the use of the Internet and technology through a communication network.

h. Data means information that can be stored in various forms within a network or computer system.

i. Bank Account means a business relationship established between a contact and a reporting organisation to enable the use of products and services of a reporting organisation. This term also includes a bank account that is used by a third party or third party company or organisation to make payments directly for business transactions for themselves or on their behalf.

j. Communication Network means a control system and infrastructure connected by wireless, wired, fiber optic, satellite or other electromagnetic system for the electronic transmission, reception, transmission or exchange of text, audio, images, video or data. This term also includes public communication networks, private networks and the Internet.

k. Social Network means an online-based service, website or software application that allows users to create, publish, share and interact with other users through a communication network.

l. Mobile Financial Services Account means a mobile financial service provider that stores a monetary value of the subscriber's mobile phone in order to provide mobile financial services.

m. Telecommunications operator means a digital development and telecommunications operator under the supervision of the Ministry, Department of Telecommunications.

n. Internet Service Provider (ISP) means a person or organisation that provides digital platform services that can be used within the country.

o. Mule Account means allowing or renting one's bank account, electronic wallet (E-wallet) or SIM CARD to be used by another person in order to transfer, hide or launder funds derived from crime.

Chapter (3) the purpose

4. The objectives of this law are as follows:

    a. To coordinate with domestic forces as well as foreign governments to prevent online fraud from taking root in the country

    b. To prevent the country's sovereignty and stability from being compromised by illegal entry into the country through border areas and committing online fraud crimes

    c. To eradicate and take action against online fraud crimes

    d. To prevent public harm caused by online fraud

e. To establish a system for exchanging information between banks and financial institutions, telecommunications service providers, and relevant government departments and organisations

f. To screen and detain foreigners who are illegally present in the area where online fraud is committed

g. To seize and manage movable and immovable property used in committing online fraud, as well as the profits derived from committing online fraud.

Chapter (4) Formation of the Central Committee and its duties and powers

5. The Union Government shall:

    a. The Central Committee for the Supervision of Combating Online Fraud shall be formed as follows:

        (a) Union Minister, Ministry of Home Affairs

        (b) Union Minister, Ministry of Foreign Affairs

        (c) Union Minister, Ministry of Immigration and Population

        (d) Chairman/Prime Minister Nay Pyi Taw Council, Region/State Government — Member

        (e) Central Bank of Myanmar — Member

        (f) Regional Commander, relevant regional headquarters — Member

        (g) Deputy Minister, Ministry of Transport — Member

        (h) Deputy Minister, Ministry of Digital Development and Communications — Member

        (i) Deputy Minister, Ministry of Defence — Member

        (j) Deputy Minister, Ministry of Home Affairs — Member

        (k) Deputy Minister, Ministry of Border Affairs — Member

        (l) Deputy Minister and Deputy Attorney General, Ministry of Legal Affairs — Member

        (m) Deputy Minister, Ministry of Information — Member

        (n) Deputy Minister, Ministry of Social Welfare, Relief and Resettlement — Member

        (o) Deputy Chief of Military Security Affairs of the Armed Forces — Member

        (p) Chief of Police, Myanmar Police Force, Ministry of Home Affairs — Secretary

(q) Deputy Chief of Police, Myanmar Police Force, Ministry of Home Affairs — Joint Secretary

(r) Head of Department, Transnational Crime Division — Joint Secretary

(s) Troop commander, Criminal Police, Myanmar Police Force, Ministry of Home Affairs — Joint Secretary

b. The Central Committee may be amended and formed if necessary.

6. The duties and powers of the Central Committee are as follows:

a. Develop and implement strategies, policies, and procedures to combat online fraud

b. Establishing committees and assigning responsibilities to combat online fraud

c. Coordinate and implement anti-online fraud activities between the Ministry of Digital Development and Communications, Ministry of Home Affairs, Ministry of Foreign Affairs, Central Bank of Myanmar, Financial Intelligence Unit and other relevant organisations

d. Collect, verify, analyse, and disseminate information on international and domestic online fraud networks to relevant organisations

e. Directing and supervising the identification and arrest of online fraud perpetrators and online fraud centres and prosecuting them in accordance with the law

f. Direct and supervise the effective legal action against online fraud leaders who commit human trafficking and forced labour

g. Combating cross-border online fraud in collaboration with regional and international organisations, including the International Police Organisation (INTERPOL) and the ASEAN Police Organisation (ASEANAPOL)

h. Confiscating and controlling money and assets obtained from online fraud

i. Systematically allocate and manage the necessary manpower, technology, and funds for anti-online fraud activities

j. Directing and supervising local committees to seize movable and immovable property used in committing online fraud, and profits derived from committing online fraud

k. Receive complaints from victims of online fraud and coordinate assistance through relevant departments (suspension of banking services, psychological support)

l. Blocking mobile telephone numbers, websites and accounts used to commit online fraud in collaboration with telecommunications operators and internet service providers

m. Establish and coordinate plans to rescue citizens and foreigners who are forced into or trapped in online fraud centres

n. Cooperating with international organisations and embassies to safely repatriate rescued people to their respective countries

o. Educating the public about the various forms of online fraud, the dangers, and ways to prevent them

p. Carrying out tasks related to combating online fraud assigned by the Union Government from time to time.

Chapter (5) Formation of Regional Committees

7. The Central Committee shall:
    a. The Region or State Online Fraud Prevention Committee shall:
        (a) …
    b. The Union Territory Online Fraud Prevention Committee is formed as follows:
        (a) …
    c. The regional committee referred to in subsections (a) and (b) may be amended and formed if necessary.
8. The responsibilities of the Regional Committee are as follows:
    a. To identify and combat online fraud until it is eradicated
    b. Forming special teams to detect and arrest online fraud
    c. Seizure of movable and immovable property used in committing online fraud, and the profits derived from committing online fraud
    d. Screening and detaining foreigners who visit places where online fraud is committed
    e. Taking effective action against offenders in accordance with the law
    f. Carrying out the responsibilities related to combating online fraud assigned by the Central Committee from time to time.

Chapter (6) Establishment of the Online Fraud Prevention Centre and its responsibilities

9. The Central Committee:
    a. The Online Fraud Prevention Centre shall be constituted as follows:
        (a) …
    b. The central department can be reorganised if necessary.
10. The functions of the centre are as follows:
    a. Establish a 24-hour emergency hotline for victims of online fraud to call and report
    b. Establish and implement an emergency telephone number, mobile application, and web application to directly interact with the public

c. Verifying complaints reported by victims

d. Recording information such as the account number, bank name, amount of money transferred, and time of transfer of the online fraud perpetrator

e. The information received will be checked within the banking system as soon as possible, and if it is found to be online fraud, it will be considered an emergency case.

f. Debit freeze the bank account number of the perpetrator of online fraud within 15 minutes.

g. Effectively block mule accounts and SIM cards used in committing online fraud

h. To prevent further loss of funds remaining in the bank account of the victim of online fraud, the victim's digital banking account number (Digital Banking Account) should be

i. Systematically establish procedures for temporarily suspending and inspecting financial flows to ensure that victims of online fraud can recover their lost funds as quickly as possible.

j. Tracking bank account numbers through which money continues to flow

k. Send basic information to the nearest police station and contact them to open a first information report.

l. Coordinate with the relevant bank to reopen the temporarily suspended bank account of the victim of online fraud.

m. Technologically monitor and identify mobile phone numbers, websites, links, and financial transaction patterns used to commit online fraud.

n. Verifying and submitting information and evidence for use as evidence in a case.

o. Issuing warnings and conducting awareness-raising activities to inform the public about the latest forms of online fraud.

p. Providing legal assistance, counselling, and support services to victims of online fraud.

q. Carrying out the responsibilities related to combating online fraud assigned by the Central Committee from time to time.

Chapter (7) Prevention

11. In mobile financial services, in relation to opening a mobile financial account through a communication network using a citizen verification card, mobile financial service providers:

    a. After fully implementing the Know Your Customer (KYC) and Customer Due Diligence (CDD) processes for the mobile money account holder, a system must be established to verify the identity of the mobile money account holder against the

original National Identification Card through the representative of the mobile money service provider.

b. If incomplete or suspicious information is found during the due diligence process for the mobile money account holder under subsection (a), the contact person due diligence process, or the citizen verification card verification, the mobile money account shall not be opened.

12. Banks and financial institutions must report suspicious financial transactions to the central office in accordance with the regulations.

13. Border security posts shall report any illegal border crossings by foreign nationals, whether by land or sea, to the Ministry of Defence, Ministry of Home Affairs, or Ministry of Immigration and Population.

14. The Centre shall:

    a. It must be monitored to ensure that there is no sale of bank accounts through telecommunications networks, no purchase of bank accounts by soliciting the financially disadvantaged, and no opening of bank accounts or mobile pay accounts using fake identity cards.

    b. It must be scrutinised to ensure that sim cards are not purchased from others and used to commit financial fraud using technology in the communication network, or that the proceeds are not transferred to foreign countries in stages.

    c. Monitor, investigate, and impersonate those who commit financial fraud on the communication network using social media, websites, and mobile applications.

    d. Technology must be enhanced to investigate and close suspicious accounts on social media.

    e. Cooperate with the Ministry of Digital Development and Communications to block websites suspected of committing crimes.

Chapter (8) Information exchange

15. The following organisations have been established to prevent and combat online fraud and suspicious accounts, financial flows, and communication information and must be exchanged through a centralised database:

    a. Banks and Financial Institutions

    b. Electronic Payment Service Providers (E-payment Service Providers)

    c. Telecommunications operators and Internet service providers.

16. Officials of banks and financial institutions:

    a. If suspicious financial transactions or suspicious activities related to online fraud are detected within our system, they must be reported to the Central Office immediately

b. If another bank inquires about a suspicious account number or transaction, the information must be shared immediately.

17. The telecommunications operator:

    a. Sim card registration information, location of use, and call details record (Call Details Record-CDR) must be maintained systematically.

    b. The information referred to in subsection (a) shall be provided immediately upon request by the Central Department.

18. Information exchanged between banks and financial institutions, electronic payment service providers, telecommunications operators and internet service providers shall be used only for the purpose of preventing and combating online fraud and shall be kept secure in accordance with data protection standards.

Chapter (9) Temporary suspension of cash flow and action taken

19. After a victim of online fraud becomes aware of their financial transaction, they can notify the relevant bank and financial institution as soon as possible and request a temporary suspension of the transaction.

20. The bank and financial institution that receives the notification under Article 19 shall, upon receipt of the notification, immediately implement a temporary suspension of the suspicious account number for a period not exceeding 72 hours.

21. Officials of the bank and financial institution shall:

    a. If a notification is received from a central government department or government agency regarding an online fraud offence under this law, the suspension of financial transactions shall be implemented immediately.

    b. Failure or delay in suspending the transfer of funds shall prevent the transfer of funds in the bank account number of the victim of online fraud.

22. A victim of online fraud may file a complaint with the Central Office within 24 hours of being notified by the bank under Article 19, either in person or through the Online Complaint Portal, detailing the incident.

23. The Centre shall:

    a. Verify the complaint and, if found to be valid, file a First Information Report (FIR) with the relevant police station against the victim of online fraud.

    b. The complaint record (Case Identifier-Case ID) must be sent to banks and financial institutions to track the flow of funds.

    c. Among the information reported in cases of online fraud, websites, social networks, bank account numbers, mobile payment accounts, and telephone numbers must be recorded, investigated, and closed to prevent further violations.

d. The flow of money lost by victims of online fraud must be investigated and closed promptly.

e. Directly connect with the ASEAN Police Force and the International Police Force to exchange information and submit reports to the Central Committee to prevent cross-border money flows.

f. Liaise with relevant countries in accordance with the Law on Mutual Assistance in Criminal Matters to recover funds obtained through online fraud in foreign banks.

24. If you report a crime of online fraud, the relevant police station will:

    a. Upon receipt of the information provided by the Central Office, the First Information Report shall be opened immediately.

    b. A copy of the first report must be submitted to the central office within two hours of the complaint being filed.

    c. Any additional information required in relation to the case shall be submitted to the Central Office and requested.

    d. The information and evidence verified by the Centre shall be submitted to the relevant court as an expert opinion.

25. If the victim of online fraud does not file a first-informant complaint during the temporary suspension period under Article 20, the relevant bank shall reopen the temporarily suspended bank account number.

26. If banks and financial institutions detect unusual cash flows or suspicious online fraud within their systems, they must temporarily suspend the bank account number without waiting for a complaint from the relevant government department, government organisation, or the victim of online fraud.

27. If a temporary suspension is made under Article 26, it must be reported immediately to the Central Department.

28. Upon receiving a report from a bank or financial institution, the Central Department shall investigate the case and, if necessary, coordinate with the Central Bank and relevant government departments and agencies to suspend the bank account number or to seize the relevant documents related to the bank account number.

Chapter (10) International cooperation

29. The Central Department may, with the approval of the Central Committee, cooperate with foreign countries, the International Police Organisation, and the ASEAN Police Organisation in the following matters regarding online fraud crimes:

    a. Exchanging information to investigate cross-border online fraud

    b. Extradition and joint investigation of offenders

c. To rescue foreigners who are being forced into online fraud centres and to repatriate them to their countries, take swift action in accordance with the law against foreigners who are arrested for illegal entry into the country and carry out deportation in accordance with the regulations

d. Cooperation on online fraud technologies and capacity building issues.

30. The Centre shall implement international cooperation agreements regarding the investigation of online fraud or the collection of evidence.

Chapter (11) Prohibitions

31. No person shall distribute or transmit false information to another person through a communication network for the purpose of committing online fraud.

32. No one shall obtain a person's personal information, image, photograph or account and impersonate that person to solicit money or property.

33. No person shall fraudulently obtain or steal a person's bank account number, mobile wallet or One Time Password (OTP) using electronic communication technology by impersonating a bank, telecommunications operator or public servant.

34. No one shall register a sim card with incorrect information, use the SIM card to obtain a bank account number, or trade bank account numbers with incorrect owner names and information in order to commit online fraud.

35. Any person who knowingly or having reason to believe that the money is obtained from committing online fraud, through his/her bank account number,

36. No one shall create, distribute or sell software, mobile devices or links that are intended to be used in online fraud.

37. No telecommunications operator or internet service provider shall, knowingly or having reason to believe, block or deny access to any website that is a fraudulent website. There shall be no failure to remove.

38. No official of a bank or financial institution shall fail to investigate or report any suspicious transaction to the Central Office.

39. No person shall allow, sell or rent a SIM card registered in his/her name to another person for the purpose of committing online fraud.

40.

a. No official of a telecommunications operator shall:

(a) SIM cards that are not registered or have incomplete information will not be provided with service.

(b) SIM cards suspected of being used in online fraud or SIM cards that make an unusually high number of calls per day will not be allowed to be used.

(c) Not to unreasonably refuse or delay requests for official information regarding online fraud or instructions to block suspicious SIM cards.

b. No employee of a telecommunications operator shall knowingly or having reason to believe that online fraud may be committed, dishonestly transfer the information of a sim card registered person to another person.

41. No person shall authorise the withdrawal of funds or destroy, conceal or transmit evidence of online fraud, knowing or having reason to believe that such fraud has been committed.

42. No person shall sell or rent his/her bank account or mobile wallet knowing or having reason to believe that another person will use it to commit online fraud.

43. No internet service provider, bank, financial institution or telecommunications operator's official will disclose the personal information of any service user. No one shall sell or transfer to a person who commits online fraud.

44. No one shall open or operate an online fraud centre.

45. No one shall commit digital currency fraud (Crypto Scam).

46. No one shall recruit or direct people to commit online fraud.

47. No person shall use violence, torture, arbitrary arrest or detention, or cruel treatment against any person for the purpose of committing online fraud.

48. No person shall:

    a. No person shall be subjected to any unlawful inducement, labour exploitation, or coercion against his or her will in order to commit online fraud.

    b. No person shall commit online fraud involving human trafficking.

49. No person shall cause another person's bank account to be frozen by falsely reporting information to harm another person.

50. No person shall attempt, aid or abet or conspire to commit any offence under this Act.

Chapter (12) Penalties

51. Whoever is convicted of violating any of the prohibitions under Articles 31, 34, 35 or 49 shall be liable to imprisonment for a term not exceeding one year and not exceeding three years and may also be fined not less than one hundred thousand kyats and not more than five hundred thousand kyats.

52. Whoever is convicted of violating any of the prohibitions contained in Articles 32, 33, 36, 37, 38, 39, 40, 41, 42, or 43 shall be liable to imprisonment for a term not less than three years and not more than seven years, and may also be fined not less than five hundred thousand kyats and not more than one thousand kyats.

53. Whoever is convicted of any offence under Articles 44, 45, 46, or 48 shall be liable to imprisonment for a term which may extend to ten years or to life imprisonment, or to death, or to fine.
54. Whoever is convicted of any offence under Article 47 shall be liable to imprisonment for a term which may extend to ten years or to life imprisonment, or to death, or to fine. If the offence results in the death of any person, the death penalty shall be imposed.
55. If any person is convicted of any offence under Article 50, he shall be liable to the punishment prescribed for the offence.
56. The court shall, on conviction of any offence under this Act, make one of the following orders:
    a. Destroying evidence used in the commission of a crime
    b. Confiscate, destroy, return to the rightful owner, or otherwise manage any property related to the crime as public property
    c. Confiscating money or property obtained from committing a crime as public property, returning it to the rightful owner, or managing it in accordance with the provisions.

Chapter (13) General

57. From the date of entry into force of this law, the Central Bank, private banks, telecommunications operators and internet service providers shall:
    a. Their systems must be connected to the central network and digital systems through data exchange technology (Application Programming Interface-API).
    b. The costs of installing automatic systems, building the necessary infrastructure, and maintaining them shall be borne by the company.
58. The central department shall establish a system for real-time monitoring of suspicious financial transactions, sim card usage, and internet protocol addresses.
59. Regarding the establishment of a centralised database:
    a. A unified dashboard must be established to provide immediate information on cybercrime incidents occurring nationwide.
    b. A system shall be established to systematically collect the phone numbers, IP addresses (Internet Protocol Address), bank account numbers, identity documents (IDs), and International Mobile Equipment Identity (IMEI) of online fraudsters and to provide them to Internet service providers and banks in real-time.
60. No person shall be prosecuted in any court, whether criminal or civil, in respect of any offence under this Act against any official of a bank or financial institution who has temporarily suspended a bank account number.

61. In the prosecution of any offence under this Act, the Central Committee or its delegate shall obtain prior permission from the local committee.

62. Notwithstanding anything contained in any existing law, any offence under this law shall be punishable only under this law.

63. In implementing the provisions of this law:

    a. The Ministry may issue necessary rules, regulations with the approval of the Union Government.

    b. The Central Committee and the Ministry may issue necessary notifications, orders, instructions and procedures.