ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதற் பிரிவு
FINANCIAL INTELLIGENCE UNIT

අංක 30, ජනාධිපති මාවත, කොළඹ 01, ශ්‍රී ලංකාව
இல. 30, சனாதிபதி மாவத்தை, கொழும்பு - 01, இலங்கை
No. 30, Janadhipathi Mawatha, Colombo 01, Sri Lanka

Guidelines No. 02/2021

Ref: 037/06/008/0006/020

July 20, 2021

To: CEOs / General Managers / Managing Directors of All Financial Institutions

Dear Madam/Sir,

Guidelines for Financial Institutions on CCTV Operations for AML/CFT Purposes, No. 2 of 2021

The above Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 06 of 2006 and the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016.

Yours faithfully,

E H Mohotty
Director/ Financial Intelligence Unit

Cc;

1. Director, Bank Supervision Department of the Central Bank of Sri Lanka
2. Director, Department of Supervision of Non - Bank Financial Institutions of the Central Bank of Sri Lanka
3. Director General, Securities and Exchange Commission of Sri Lanka
4. Compliance Officers, all Financial Institutions

☎ 011-2477125 011-2477509 | 011-2477692 011-2477708 | flu@cbsl.lk dflu@cbsl.lk | www.flusrilanka.gov.lk

Guidelines for Financial Institutions on CCTV operations for AML/CFT purposes, No. 2 of 2021

PART I

Introduction

1. These Guidelines are issued pursuant to section 15(1)(j) of the Financial Transactions Reporting Act, No. 06 of 2006 (hereinafter referred to as FTRA).

2. These Guidelines are applicable to Financial Institutions (hereinafter referred to as FIs) that are engaged in or carrying out "finance business" as defined in Section 33 of the FTRA where closed-circuit television (hereinafter referred to as CCTV) systems are being used where relevant.

3. These Guidelines should be read along with the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016, issued by Gazette Extraordinary No. 1951/13, dated January 27, 2016 (hereinafter referred to as CDD Rules). More specifically, these Guidelines should be referred together with Rules 7 and 11 of the CDD Rules, to take measures specified therein for the purpose of having proper risk control and mitigation measures by having internal policies, controls and procedures to manage and mitigate money laundering and terrorist financing risks and affiliating and integrating Financial Institution's money laundering and terrorist financing risk management with the overall risk management relating to the Financial Institution.

4. These Guidelines are issued in addition to the operational directives or circulars that are issued by the respective sector regulators with regard to CCTV systems.

5. These Guidelines are not intended to be exhaustive and do not constitute legal advice from the Financial Intelligence Unit. Nothing in these Guidelines should be construed as relieving FIs from any of their obligations under the FTRA and regulations and rules issued thereunder.

Part II

The Requirements for CCTV Systems

6. As part of the constant commitment to enhance operational risk management and safeguard banking operations against risks of being abused for money laundering and financing of terrorism, every FI is advised to have in place a robust CCTV system installed fully operational both within and outside of the premises. The business premises refer to the head office, branches, areas of Automated Teller Machines, Cash Recycling Machines and Cash deposit Machines (ATM/CRM/CDM), cash centers, outlets, and any other place or places where Customer Due Diligence (hereinafter referred to as CDD) is conducted.

7. In ensuring the CCTV system installed is effective to enable proper surveillance and monitoring of the business operations, all FIs should consider setting up a system of necessary standard with proper processes and controls, which could, at a minimum, cover the requirements set in in these Guidelines.

Placement of CCTV cameras

8. In order to enhance the effective usage of the CCTV system, FIs need to ensure that CCTV cameras are installed at appropriate locations, in a manner that the camera is able to clearly capture, monitor and record the relevant areas where business operations take place. These locations are required to include the counters, customer interaction areas where CDD takes place, areas where safe deposit boxes are located, safe or vault and other cash handling areas, ATMs/CDMs, vehicle parking areas, the entrance and exit of the business premises, any other suitable areas, both inside and outside the building as determined by the FI.

9. The CCTV surveillance systems must be aligned in a suitable manner and at an angle as to obtain a complete and unimpeded view of the area. Further, CCTVs need to be positioned in a manner where the capturing and processing information of the CCTV system is not interfered or impeded by internal or external lighting, glare, or any object.

Functions of CCTV system

10. FIs should ensure all images captured and recorded by the CCTV cameras are visible, recognizable and clear. The visual images or videos rendered through the CCTV cameras need to have the capability of identifying the features of the individuals, if any, that transact and should be clearly discernible from one image from another. In addition, adequate lighting must be maintained in order to capture clear CCTV footage.

11. Higher quality digital equipment should be used in CCTV systems to capture a clear frontal images of individuals. The CCTV systems should permit easy viewing, recording and retrieval

of high-quality images (e.g., adequate number of pixels for improved zoom capabilities) of all information contained in CCTV system. Necessary technical specifications (e.g., resolution, frame rate) need to be maintained at a standard level to achieve an effective CCTV surveillance.

12. The CCTV systems of ATMs/CRMs/CDMs should remain operational throughout the 24-hours of a day - every day of the year, including during times when the FI is closed for business.

Real time monitoring

13. FIs should ensure real-time monitoring at the head office and/or branches or at a central monitoring unit, as far as practicable.

14. FIs are advised to obtain assistance of its security services personnel or law enforcement agencies (LEAs) to mitigate immediate risks that may arise to the FI's premises or to equipment, to its customers or to potential customers, or to any person at the vicinity of the CCTV camera, if such risk is detected based on CCTV footage obtained on real-time basis.

Maintenance of records

15. FIs should maintain all information captured in the CCTV system for a minimum period of 180 days.

16. FIs, at their discretion, may retain the CCTV recordings relevant to observed suspicious activities for a longer period.

17. The FIU, LEAs or any other competent authority would, from time to time, instruct the FIs to retain the CCTV recordings relevant to a Suspicious Transactions Report furnished to FIU or any other related CCTV footage of a possible offending until the relevant investigations are concluded by the LEAs or other relevant competent authorities.

18. The FIs should ensure that its CCTV system(s) are capable of transferring the information to data storage devices, to allow retrieving and viewing of the CCTV records on electronic apparatus, such as computers.

19. To confirm the credibility of the CCTV records, FIs should ensure the timing of CCTV recording is properly set, synchronized and is consistent with the time and date of the operations that takes place at the business premises.

System administration and maintenance

20. FIs are expected to allocate adequate resources for CCTV monitoring systems, and sufficiently train the authorized personnel and staff to operate the CCTV system.

21. In order to ascertain effective surveillance and monitoring of business operations, FIs should ensure that the CCTV system(s) deployed is/are properly maintained and operational, and remain under good working condition at all times.

22. The CCTV system should be equipped with the relevant features and functions to enable to implement control measures that will prevent such system from being manipulated or misused by any unauthorized parties.

23. FIs need to ensure that all information and records of the CCTV systems maintained safely and securely without unauthorized access and adequate controls are in place to prevent unauthorized alterations of records and access by unauthorized parties, by designating and appointing officers with appropriate responsibility and authorization levels, limiting system access only to relevant personnel to ensure proper accountability for the assigned functions.

24. FIs are expected to have procedures and mechanisms to ensure that regulators, LEAs and the FIU are able to obtain information and records in relation to money laundering investigations and prosecution upon request without delay.

25. FIs are required to issue internal operational guidelines on placement, functionality, monitoring, record keeping, system maintenance and administration, and include it as a part of AML/CFT policy as well with the approval of BOD.

26. Procedures should be in place for periodical review and audit of the CCTV system(s) for number of existing cameras in the premises at branch level and where standalone ATM/CDM are located. Audits and reviews should ensure the adequacy of the number of cameras, functionality, accuracy, operability, record keeping and other salient requirements. A report of such review/ audit on the adequacy of CCTV coverage should be submitted to the Board of Directors (BOD) and to the senior management.

27. Based on the report submitted to the BOD, if the quality and coverage of CCTV systems are inadequate or more quality and coverage is desired, the senior management and the BOD are advised to take appropriate steps to rectify such deficiency or increase the coverage as appropriate. Further, immediate steps should be taken to replace or upgrade the equipment soon after any malfunction is detected.

28. FIs should ensure activities relating to the maintenance and recalibration of the CCTV system including system upgrading, reformatting and removal of records are clearly recorded in the system's maintenance log and reported to the senior management, as appropriate.