Annex F

Draft Notice to Licensed Credit Bureaus on Cyber Hygiene

THIS VERSION OF THE NOTICE IS IN DRAFT FORM AND IS SUBJECT TO CHANGE.

MAS Notice No.: [To be published]

Issue Date: [To be published]

NOTICE TO LICENSED CREDIT BUREAUS
CREDIT BUREAU ACT 2016 (ACT 27 OF 2016)

NOTICE ON CYBER HYGIENE

---

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 75(1) of the Credit Bureau Act 2016 (the "Act") and applies to all licensed credit bureaus.

2 DEFINITIONS

2.1 For the purpose of this Notice —

"administrative account", means any user account, that has full privileges and unrestricted access to any one or more of the following systems:

(a) an operating system;
(b) a database;
(c) an application;
(d) a security appliance; or
(e) a network device;

"critical system" in relation to a licensed credit bureau, means a system, the failure of which will cause significant disruption to the operations of the licensed credit bureau or materially impact the licensed credit bureau's service to a relevant person such as a system which –

(a) processes transactions that are time critical; or
(b) provides essential services to relevant persons;

"customer" has the same meaning as in section 2 of the Act but includes any company that carries on banking business, or such other financial institution as may be prescribed for the purposes of the definition of "customer" in section 2 of the Act;

"multi-factor authentication" means the use of two or more factors to verify an account holder's claimed identity. Such factors include, but are not limited to:

(a) something that the account holder knows such as a password or a personal identification number;

(b) something that the account holder has such as a cryptographic identification device or token;

(c) something that the account holder is such as an account holder's biometrics or his behaviour;

"relevant person" means a customer, data subject, or member;

"relevant person information" means any information relating to, or any particulars of, any relevant person, where a named relevant person or group of named relevant persons can be identified, or is capable of being identified, from such information;

"security patch", in relation to a system, means an update that can be applied to the system to address a vulnerability;

"security standards", in relation to a system, means a set of configurations for the purpose of safeguarding and improving the security of the system;

"system", in relation to a licensed credit bureau, means any hardware or software that is used by the licensed credit bureau;

"vulnerability", in relation to a system, means any weakness, susceptibility or flaw of the system that can be exploited, including but not limited to by allowing an unauthorised person to access the system, or to compromise the security configuration settings of the system.

2.2 Any expression used in this Notice shall, except where expressly defined in this Notice or where the context requires, have the same meaning as in the Act.

3 APPLICATION OF NOTICE

3.1 A licensed credit bureau need not comply with a requirement in this Notice to the extent that it is unable to exercise control over a system to ensure compliance with that requirement, in all of the following ways:

(a) the licensed credit bureau cannot exercise direct control over the system to ensure compliance with that requirement;

(b) a licensed credit bureau cannot exercise indirect control over the system by requiring the system provider to ensure compliance with that requirement;

(c) it is not reasonable for the licensed credit bureau to procure an alternative system provider over whom the licensed credit bureau is able to exercise such indirect control referred to in sub-paragraph (b), to provide the system.

4 CYBER HYGIENE PRACTICES

4.1 **Administrative Accounts**: A licensed credit bureau must ensure that every administrative account in respect of any operating system, database, application, security appliance or network device, is secured to prevent any unauthorised access to or use of such account.

4.2 **Security Patches**:

(a) A licensed credit bureau must ensure that security patches are applied to address vulnerabilities to every system, and apply such security patches within a timeframe that is commensurate with the risks posed by each vulnerability.

(b) Where no security patch is available to address a vulnerability, the licensed credit bureau must ensure that controls are instituted to reduce any risk posed by such vulnerability to such a system.

4.3 **Security Standards:**

(a) A licensed credit bureau must ensure that there is a written set of security standards for every system.

(b) Subject to sub-paragraph (c), a licensed credit bureau must ensure that every system conforms to the set of security standards.

(c) Where the system is unable to conform to the set of security standards, the licensed credit bureau must ensure that controls are instituted to reduce any risk posed by such non-conformity.

4.4 **Network Perimeter Defence:** A licensed credit bureau must implement controls at its network perimeter to restrict all unauthorised network traffic.

4.5 **Malware Protection**: A licensed credit bureau must ensure that one or more malware protection measures are implemented on every system, to mitigate the risk of malware infection, where such malware protection measures are available and can be implemented.

4.6 **Multi-factor Authentication:** Subject to paragraph 4.7, a licensed credit bureau must ensure that multi-factor authentication is implemented for the following:

(a) all administrative accounts in respect of any operating system, database, application, security appliance or network device that is a critical system; and

(b) all accounts on any system used by the licensed credit bureau to access relevant person information through the internet.

4.7 (a) Paragraph 4.6 shall not apply to a licensed credit bureau for the period between [effective date of Notice] to [end of 6 months from effective date of Notice] (both dates inclusive), if the licensed credit bureau meets all of the following conditions:

(i) the licensed credit bureau identifies all the risks or potential risks posed by its non-compliance with paragraph 4.6 during that period;

(ii) the licensed credit bureau implements controls to reduce the risks identified in sub-paragraph (i);

(iii) a committee of the licensed credit bureau, or a member of the senior management of the licensed credit bureau –

(A) agrees with the risk assessment in sub-paragraph (i); and

(B) is satisfied that the controls to be implemented in subparagraph (ii) are adequate to reduce the risks identified in sub-paragraph (i).

(b) In this paragraph —

"committee of the licensed credit bureau" means a group of persons that:

(i) comprises at least 2 persons, each of whom is a person who is not a member of the senior management of the licensed credit bureau but is concerned with or takes part in the management of the licensed credit bureau on a day-to-day basis; and

(ii) is appointed by a member of the senior management of the licensed credit bureau to –

(A) assess the risks or potential risks posed by the licensed credit bureau's non-compliance with paragraph 4.6 during the period

between [effective date of Notice] to [end of 6 months from effective date of Notice]; and

(B) approve the implementation of the controls to reduce the risks posed by the non-conformity with paragraph 4.6.

"member of the senior management" means a person for the time being holding the office of chief executive officer or an equivalent person of the licensed credit bureau and includes a person carrying out the duties of any such office if the office is vacant.

Effective Date

5 This Notice shall take effect on [date of Act commencement].