

Date: 12 December 2025

Cybersecurity Incident Notification

- 1 The National Credit Regulator (NCR) has been the victim of a cyber-attack that has caused disruption to certain systems.
- 2 As is common with cyber incidents of this nature, we do not know the identities of the individuals responsible for this criminal conduct.
- 3 Upon detecting unusual activity, our teams acted swiftly in line with established incident response protocols. These measures included isolating affected systems, disabling remote access, and implementing enhanced security controls to contain the threat and minimise further disruption.
- 4 Recognising the seriousness of this event, we engaged independent cybersecurity specialists to assist with investigation and recovery efforts. We are working towards restoring our environment securely to ensure the continuity of our operations.
- 5 We have notified the relevant government and regulatory authorities, including the Information Regulator, to ensure compliance with legal requirements.
- 6 Our investigation remains ongoing to verify the accuracy of the claims made by the criminal third parties and to determine the nature of the data involved, including the extent to which personal information is affected.
- 7 We urge all stakeholders to remain vigilant during this time:
 - (a) Exercise extreme caution with any suspicious emails or messages.
 - (b) Do not click on unknown or unexpected links.
 - (c) Be wary of any unusual communications claiming to be from the NCR.
 - (d) Consider applying for Protective Registration with the Southern African Fraud Prevention Service (SAFPS). This is free and adds an extra layer of protection against identity fraud.
- 8 Our priority remains to restore our systems securely and maintain continuity of essential services. We are committed to safeguarding the interests of our stakeholders. Further updates will be shared as our investigation progresses.
- 9 For any queries, please contact Enquiries@ncr.org.za.