Office of RBI Ombudsman https://cms.rbi.org.in/ 25 General precautions ➢ Be wary of suspicious looking pop ups that appear during your browsing sessions on internet. ➢ Always check for a secure payment gateway (https:// - URL with a pad lock symbol) before making online payments / transactions. ➢ Keep the PIN (Personal Identification Number), password, and credit or debit card number, CVV, etc., private and do not share the confidential financial information with banks/ financial institutions, friends or even family members. ➢ Avoid saving card details on websites / devices / public laptop / desktops. ➢ Turn on two-factor authentication where such facility is available. ➢ Never open / respond to emails from unknown sources as these may contain suspicious attachment or phishing links. ➢ Do not share copies of chequebook, KYC documents with strangers. For device / computer security ➢ Change passwords at regular intervals. ➢ Install antivirus on your devices and install updates whenever available. ➢ Always scan unknown Universal Serial Bus (USB) drives / devices before usage. ➢ Do not leave your device unlocked. ➢ Configure auto lock of the device after a specified time. ➢ Do not install any unknown applications or software on your phone / laptop. ➢ Do not store passwords or confidential information on devices. Office of RBI Ombudsman https://cms.rbi.org.in/ 26 For safe internet browsing ➢ Avoid visiting unsecured / unsafe / unknown websites. ➢ Avoid using unknown browsers. ➢ Avoid using / saving passwords on public devices. ➢ Avoid entering secure credentials on unknown websites/ public devices. ➢ Do not share private information with anyone, particularly unknown persons on social media. ➢ Always verify security of any webpage (https:// - URL with a pad lock symbol), more so when an email or SMS link is redirected to such pages. For safe internet banking ➢ Always use virtual keyboard on public devices since the keystrokes can also be captured through compromised devices, keyboard, etc. ➢ Log out of the internet banking session immediately after usage. ➢ Update passwords on a periodic basis. ➢ Do not use same passwords for your email and internet banking. ➢ Avoid using public terminals (viz. cyber cafe, etc.) for financial transactions. Office of RBI Ombudsman https://cms.rbi.org.in/ 27 Factors indicating that a phone is being spied ➢ Unfamiliar applications are being downloaded on the phone. ➢ There is a faster than usual draining of phone battery. ➢ Phone turning hot may be a sign of someone spying by running a spyware in the background. ➢ An unusual surge in the amount of data consumption can sometimes be a sign that a spyware is running in the background. ➢ Spyware apps might sometimes interfere with a phone’s shutdown process so that the device fails to turn off properly or takes an unusually long time to do so. ➢ Note that text messages can be used by spyware and malware to send and receive data. Actions to be taken after occurrence of a fraud ➢ Block not only the debit card / credit card but also freeze the debit in the bank account linked to the card by visiting your branch or calling the official customer care number available on the bank’s website. Also, check and ensure the safety of other banking channels such as Net banking, Mobile banking etc., to prevent perpetuation of the fraud once the debit/ credit cards, etc., are blocked following a fraud. ➢ Dial helpline number 155260 or 1930 or report the incident on National Cybercrime Reporting Portal (www.cybercrime.gov.in). Reset Mobile: Use (Setting-Reset-Factory Data) to reset mobile if a fraud has occurred due to a data leak from mobile. Precautions related to Debit / Credit cards ➢ You should deactivate various features of credit / debit card, viz., online transactions both for domestic and international transactions, in case you are not going to use the card for a while and activate the same only when the card usage is required. ➢ Similarly, Near Field Communication (NFC) feature should be deactivated, if the card is not to be used. ➢ Before entering PIN at any Point of Sale (POS) site or while using the card at an NFC reader, you must carefully check the amount displayed on the POS machine screen and NFC reader. Office of RBI Ombudsman https://cms.rbi.org.in/ 28 ➢ Never let the merchant take the card away from your sight for swiping

while making a transaction. ➢ Cover the keypad with your other hand while entering the PIN at a POS site / ATM. For E-mail account security ➢ Do not click on links sent through emails from unknown addresses / names. ➢ Avoid opening emails on public or free networks. ➢ Do not store secure credentials / bank passwords, etc., in emails. For password security ➢ Use a combination of alphanumeric and special characters in your password. ➢ Keep two factor authentication for all your accounts, if such facility is available. ➢ Change your passwords periodically. ➢ Avoid having you date of birth, spouse name, car number etc. as passwords. Office of RBI Ombudsman https://cms.rbi.org.in/ 29 How do you know whether an NBFC accepting deposit is genuine or not? ➢ Verify whether the name of NBFC appears in the list of deposit taking NBFCs entitled to accept deposits, available at https://rbi.org.in and to ensure that it is not appearing in the list of companies prohibited from accepting deposits. ➢ NBFCs must prominently display the Certificate of Registration (CoR) issued by the Reserve Bank on its site / in its office. This certificate should also reflect that the NBFC has been specifically authorised by RBI to accept deposits. Scrutinize the certificate to ensure that the NBFC is authorised to accept deposits. ➢ NBFCs cannot accept deposits for a period less than 12-months and more than 60 months and the maximum interest rate that an NBFC can pay to a depositor should not exceed 12.5%. ➢ The Reserve Bank publishes the change in the interest rates on https://rbi.org.in → Sitemap → NBFC List → FAQs.