FREQUENTLY ASKED QUESTIONS

1. **When and how did you notice the attack?**
   We identified the attack in the past week through our internal controls.

2. **What type of information was compromised?**
   Information compromised consisted of card and linked account numbers, card expiry dates and card holder names of our customers. There is no evidence that any of our customers' financial information or personal information was compromised.

3. **Will you renew the cards?**
   Our cards are secure and customers can continue to use their cards as usual.

4. **Can the stolen information be used to print cards and withdraw money from ATMs?**
   No. It is not possible to print cards and withdraw money from ATMs with the compromised information.
   Our customers can continue to use their cards confidently.

5. **Is it possible to use the stolen information to make transactions through internet banking or telephone banking?**
   No. It is not possible to make any transactions through internet banking or telephone banking with the compromised information. Our customers can continue to use internet banking and telephone banking confidently.

6. **Are my current accounts/term deposit accounts safe?**
   Yes. Only the linked account number was compromised. The content of the account was not compromised. It is not possible to commit fraud with the linked account number. This information is regularly shared by our customers with the 3rd parties when they make money transfers and EFT transactions. No other information was compromised, including account numbers of term deposit accounts or other deposit accounts.

7. **Was any other information compromised?**
   No. There is no evidence that any other information was compromised.

8. **Have you noticed any fraud or suspicious transactions resulting from this incident?**
   No. We have not identified any fraud or suspicious transactions resulting from this incident.

9. **Will the bank reimburse any possible losses?**
   Yes. If any confirmed fraudulent transactions occur related to this incident, we will reimburse our customers.

10. **What kind of precautions and actions are you taking to prevent this from happening again?**
    The HSBC Group takes the security of its customers' information extremely seriously and constantly reviews systems and security. We are leveraging the strength of HSBC's global network and security expertise to take swift and decisive action. On identifying the incident we immediately implemented enhanced security measures to improve the security of our information systems and card transactions.

HSBC

11. **Do you have any information about the attackers?**
    Investigations are ongoing in collaboration with the Banking Regulation and Supervision Agency of Turkey (BRSA) and other relevant authorities. We have also notified Public Prosecutor's Office.

12. **Do you recommend any further precautions for your customers?**
    Our customers do not need to take any action as a result of this incident and they can confidently continue their banking transactions. As usual, we would like to remind our customers that they should ensure all normal precautions are undertaken with their cards, use reliable online shopping sites, monitor card usage and inform the bank if they suspect any fraudulent activities on their cards.

13. **Why have they taken this information if they are unable to commit fraud?**
    We cannot speculate on the intent of the attackers. We are confident that there is no financial risk to our customers and there has been no evidence of any fraud or other suspicious activity arising from this incident.

14. **Will this effect HSBC's operations in other countries?**
    This attack is limited to HSBC Turkey.

HSBC