Please note this is an in-depth version of the ideal answer. We have included additional information in this document to help you understand the thinking and rationale behind the sample solution!

I. Draft E-Mail to client

Dear Mr. Dent,

thank you for the information provided to us. We have assessed if there is any notification obligation for Great New Games under the EU General Data Protection Regulation ("**GDPR**") regarding the data leak occurred. We understand that the customer database operated by Great New Games containing information on names, addresses and credit card information has been unencrypted and the information have therefore been available to public access for a period of up to six days. However, Great New Games has no evidence that any unauthorised database access has occurred.

Ultimately, to our understanding, Great New Games is obliged to notify (1.) the competent supervisory authority and (2.) Great New Games' customers affected about the data leak. In case of a violation of these obligations, GDPR provides for fines of up to EUR 10,000,000 or up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (3.). Therefore, as requested, we have prepared the necessary notification letters (see attached). The supervisory authority should be notified as soon as possible.

1. Notification obligation to the competent authority

As per Art. 33 para 1 s. 1 GDPR, the controller is obliged to notify the supervisory authority about a personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

a) Controller

According to Art. 4 Nr. 7 GDPR controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art. 4 Nr. 2 GDPR). Great New Games is the legal person determining the purpose of the storage and the use of customers' data in the context of the operation of the web shop. Thus, Great New Games is controller pursuant to Art. 4 Nr. 7 GDPR.

b) Personal data breach

The data leak constitutes a personal data breach. Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, Art. 4 Nr. 12 GDPR. Due to the data leak, customer information was publicly available and therefore disclosed without authorisation.

It is irrelevant that there is no evidence of actual data access by third parties. The personal data breach has already occurred as the data was publicly available. This conclusion is supported by the definition of "processing" in Art. 4 Nr. 2 GDPR: Making personal data available is sufficient to fulfil the definition of processing. Thus, making data available without permission to third parties regardless of actual data access leads to a data breach. The probability of unauthorised data access must be taken into account within the risk assessment.

c) Likeliness of a risk to the rights and freedoms of natural persons

A notification obligation does not apply if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. One could argue that, as there is no evidence of unauthorised data access by third parties, it is unlikely that the data leak will result in a risk to the rights and freedoms of natural persons. However, the sensitivity of the data held in the database must be taken into account. If the consequences of potential third party data access are of great significance for the customer, the requirements regarding the likeliness of a damage to the rights and freedoms of natural persons are lowered.

During the data leak, credit card information has been made available. Third parties could abuse this information to the customers' disadvantage leading to identity fraud and financial loss (cf. recital 85 GDPR). Therefore, even if the likeliness of a risk to the rights and freedoms of natural persons could be deemed rather low, the consequences are of great importance to Great New Games' customers. So, to our understanding, the exemption to the notification obligation set out in Art. 33 para 1 s. 1 GDPR is not applicable. Thus, Great New Games is obliged to notify the supervisory authority about the personal data breach.

d) Notification obligation

The notification obligation must be fulfilled within 72 hours after Great New Games became aware of the personal data breach. Art. 33 para 3 GDPR sets out the necessary content of such a notification. The notification shall at least

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by Great New Games to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In addition, as per Art. 33 para 5 GDPR, Great New Games is obliged to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. This documentation will have to be made available to the supervisory authority.

2. Notification obligation to customers

Pursuant to Art. 34 para 1 GDPR, the controller shall communicate the personal data breach to the data subject without undue delay in case the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. As laid out above, Great New Games is controller under the GDPR and a personal data breach in the sense of Art. 34 para 1 GDPR has occurred. Contrary to Art. 33 para 1 GDPR, a notification obligation is only applicable in case the data breach leads to a high risk to the rights and freedoms of natural persons.

a) High risk to the rights and freedoms of natural persons

As set out above, the higher the potential risk to the rights and freedoms of natural persons, the lower the requirements regarding the likeliness of an actual damage are. Again, one could argue that there

is no evidence of unauthorised data access, but the potential consequences to Great New Games' customers remain of high significance. Recital 85 to the GDPR underlines the importance of data breach cases that potentially lead to identity theft or fraud and financial losses. In case of potential disclosure of credit card information, customers face a high risk of data abuse and financial loss. We therefore deem it likely that this case would be considered a case of high risk to the rights and freedoms of natural persons.

In addition, Great New Games' risk assessment should take into account the potential fines of significant amount under Art. 83 GDPR (s. below).

b) Exemptions

Art. 34 para 3 GDPR provides for several exemptions from the notification obligation. A notification to the data subject is not required if

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
- it would involve disproportionate effort.

To our understanding, none of these exemptions are applicable. The customer data has already been publicly available so that subsequent protection measures do not mitigate the risk to the customers that has already arisen. The notification of the data subjects affected would, in addition, not involve disproportionate effort as the customers and contact options are known so they can be easily notified.

Consequently, to our understanding Great New Games is obliged to notify the affected customers about the data leak.

c) Notification obligation

Pursuant to Art. 34 para 2 GDPR, the notification of the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the following information:

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- likely consequences of the personal data breach;
- measures taken or proposed to be taken by Great New Games to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

3. Legal enforcement

Violations of the notification obligations are subject to administrative fines as per Art. 83 para 4 GDPR. The fines can amount up to 10,000,000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

If you have any further questions, please feel free to contact us.

Kind regards

[…]