Some explanatory notes concerning the data breach notification to the supervisory authority, based on Guidelines 01/2021 on Examples regarding Personal Data Breach Notification Adopted on 14 December 2021 Version 2.0

Concerning question 1.1., please see:

"5. In its Opinion 03/2014 on breach notification4 and in its Guidelines WP 250, WP29 explained that breaches can be categorised according to the following three well-known information security principles:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.

- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

6. A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals. One of the most important obligation of the data controller is to evaluate these risks to the rights and freedoms of data subjects and to implement appropriate technical and organizational measures to address them."[1]

Concerning questions in section 4 please see:

The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject. Controllers should make this assessment at the time they become aware of the breach. The controller should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether or not the data breach is likely to result in a risk and thus should be notified.

Concerning question 9.3 please see:

"3.3 CASE No. 07: Credential stuffing attack on a banking website

A bank suffered a cyber-attack against one of its online banking websites. The attack aimed to enumerate all possible login user IDs using a fixed trivial password. The

[1] Guidelines, p. 6.

passwords consist of 8 digits. Due to a vulnerability of the website, in some cases information regarding data subjects (name, surname, gender, date and place of birth, fiscal code, user identification codes) were leaked to the attacker, even if the used password was not correct or the bank account not active anymore. This affected around 100.000 data subjects. Out of these, the attacker successfully logged into around 2.000 accounts which were using the trivial password tried by the attacker. After the fact, the controller was able to identify all illegitimate log-on attempts. The data controller could confirm that, according to antifraud checks, no transactions were performed by these accounts during the attack. The bank was aware of the data breach because its security operations centre detected a high number of login requests directed toward the website. In response, the controller disabled the possibility to log in to the website by switching it off and forced password resets of the compromised accounts. The controller communicated the breach only to the users with the compromised accounts, i.e. to users whose passwords were compromised or whose data was disclosed.

3.3.1 CASE No. 07 - Prior measures and risk assessment

63. It is important to mention that controllers handling data of highly personal nature21 have a larger responsibility in terms of providing adequate data security, e.g. having a security operation's centre and other incident prevention, detection and response measures. Not meeting these higher standards will certainly result in more serious measures during an SA's investigation.

64. The breach concerns financial data beyond the identity and user ID information, making it particularly severe. The number of individuals affected is high.

65. The fact that a breach could happen in such a sensitive environment points to significant data security holes in the controller's system, and may be an indicator of a time when the review and update of affected measures is "necessary" in line with Articles 24 (1), 25 (1), and 32 (1) of the GDPR. The breached data permits the unique identification of data subjects and contains other information about them (including gender, date and place of birth), furthermore it can be used by the attacker to guess the customers' passwords or to run a spear phishing campaign directed at the bank customers.

66. For these reasons, the data breach was deemed likely to result in a high risk to the rights and freedoms of all the data subjects concerned22. Therefore, the occurrence of material (e.g. financial loss) and non-material damage (e.g. identity theft or fraud) is a conceivable outcome."[2]

[2] Guidelines, p. 18.