SLIDE 5

Risk assessment: What factors should be considered?

- Could individuals be identified from the information compromised?

Also look at how easily someone with access to the data compromised could identify who it related to? Now this could be possible directly from the information disclosed, or it could be difficult to match the data to a

- Is the incident contained?

Is the incident contained? Consider whether the data is back under the control of the organisation. Has the unintended recipient confirmed they have securely destroyed or deleted the information? Has the data been located that was thought to be lost? Have laptops been remotely wiped when stolen, or have system passwords been changed?

- What actions have been taken to mitigate the severity of the consequences?

Finally consider if there are any further actions you can take aside from containment to mitigate the severity of the possible consequence. This could be anything from providing support to a destressed individual, or giving the data subjects guidance on measures they can take to protect themselves.

SLIDE 9

Assessing Breaches

We will now go through the things you will need to consider when you are assessing breach reports. You should keep in mind that your decisions should be made on a case-by-case basis. These are the factors you should take into account when reviewing reports received to decide what action we will take. In most cases we aim to close with advice but if it is a severe breach then we would look at referring cases for further enforcement action.

- **How has the breach happened? –** Looking at the root cause of how an incident has occurred could help you to establish whether further action needs to be taken. Was this a result of human error or were there inadequate processes in place. Did the controller know they should have better security in place but fail to implement proper measures, or did they fail to consider the risks that could arise in respect of the personal information they were processing?

- **What measures did the controller have in place to prevent the breach?** – This is one of the main areas to consider when assessing a breach report. Did the controller have the appropriate security measures in place to protect the personal data that is being processed. For example, if an organisation is processing sensitive information like gender reassignment information, we would expect the security to be stronger than if they only handled email addresses. Essentially, we will be looking at whether their security was fit for purpose.

- **Action taken by an organisation in response to a breach –** An organisations response to an incident is important factor when assessing a breach report. What steps have they taken to contain the breach and reduce the risks for individuals? Has action been taken to mitigate for example have they added credit monitoring to an individual's account. Is the organisation reviewing their processes or staff training to make improvements and prevent a reoccurrence.

- **Any previous breaches by the controller?** Has the controller experienced similar incidents before? We should note whether the ICO has previously provided advice to the controller which, if that advice had been followed, could have prevented the breach from recurring.

When picking up a case you will need to take into consideration all of these factors in order to decide what action to take.