ICO Notification Submitted? What Next? Other Bodies To Consider Notifying.

Published 24 June 2021

In May's edition of the Data and Cyber Bulletin we explored the key considerations for an organisation following a data breach. We noted the importance of notifying the ICO within 72 hours of an organisation becoming aware of a personal data breach. However, the ICO is not the only body to which an organisation can be obligated to notify following a data breach. Consequently, this month we will focus on the other organisations you may need to notify following a data breach, although we note this is not an exhaustive list.

1. Financial Conduct Authority ("FCA")

Principle 11 of the FCA Handbook states that firms must disclose to the FCA anything relating to the firm of which the FCA would reasonably expect notice. It is established that material cyber incidents meet this threshold. A cyber incident is likely to be material if:

- A significant amount of data is lost, or a firm's availability and/or control of its IT systems is impacted;
- A large proportion of customers are affected; or
- The cyber attack results in unauthorised access to, or malicious software is found on, your firms information and communication systems.

Payment service providers should additionally note their obligations to make a notification following major operational or security incidents under the Payment Services Regulations 2017.

2. Prudential Regulation Authority ("PRA")

The Bank of England regulates and supervises financial firms through the PRA. The PRA has eight Fundamental Rules which are similar to the FCA's Principles for Businesses. Of particular note is Fundamental Rule 7 which mirrors Principle 11 of the FCA Handbook and obligates firms to be open and cooperative and disclose to the PRA matters of which the PRA would reasonably expect notice. As was considered above, if your firm is regulated by the PRA and has suffered from a cyber incident, assess whether the severity of incident is material enough that the PRA should be notified.

3. Action Fraud

If your organisation is the victim of a cyber incident perpetuated by a criminal, you should also consider reporting the breach to Action Fraud. Action Fraud is the UK's national centre for reporting fraud and cybercrime. All reports are passed on for assessment by the National Fraud Intelligence Bureau who may then send them to police forces for investigation. Others may be sent to Action Fraud's Prevention and Disruption Team where the fraud enabler i.e. a telephone number or website address, can be blocked to prevent other organisations from falling victims to the same cyber attack.

If you are in Scotland then reports should be made to Police Scotland.

4. National Cyber Security Centre ("NCSC")

Cyber incidents may also need to be notified to the NCSC. The NCSC provides advice, guidance and support on cyber security and the management of cyber security incidents. The NCSC seeks to reduce the harm caused to victims of cyber attacks and uses the knowledge gained through notifications to update its guidance to help deter future attacks. It traditionally assists organisations with cyber incidents of national importance.

However, where there is a severe cyber incident, the NCSC may be able to:

- Provide technical advice and guidance;
- Use its knowledge of similar incidents to understand the data breach. This could include identifying the threat actor, its likely motive, any other organisations which may be targeted and if the compromise is likely to spread; or
- Coordinate any cross-government response.

5. The Network and Information Systems Regulations 2018 ("NIS Regulations")

If your organisation is an Operator of Essential Services, as defined under the NIS Regulations, then you should also consider whether you need to inform your Competent Authority of the cyber incident.

Overall, notifying organisations of a cyber incident is important for not only your organisation but also for the public and national authorities. It allows for the collection of data to understand cybersecurity trends, identify common weaknesses, common modes of attack and provide guidance to prevent similar attacks from occurring in the future.

Authors

DAC BEACHCROFT