Alerts and Updates

TOUGHER PENALTIES FOR BREACH OF UK DATA PROTECTION LAWS

January 13, 2010

The Information Commissioner's Office (ICO)—the United Kingdom's data regulator—announced in a 12 January 2010 release that new powers designed to fine organizations responsible for security breaches are likely to come into effect on 6 April 2010. From that date forward, fines of up to £500,000 can be imposed on organizations for what are considered serious breaches of the UK's Data Protection Act 1998.

For the fine to be levied, "the Information Commissioner must be satisfied that there has been a serious breach that was likely to cause damage or distress and it was either deliberate or negligent and the organisation failed to take reasonable steps to prevent it." The ICO provided examples of when the new powers will be used, such as when customers face identity theft following a data breach or when an organization collects data for a competition but then uses the entrant's details for other purposes. The legislation states that an enforcement notice can be issued at the same time as a fine. In the past, enforcement notices that were served required a corporation to encrypt laptops after a breach, change its marketing practices or take other compliance measures.

The new UK powers are likely to strengthen compliance requirements for multinational organizations. While these powers are similar in some respects to US data breach laws, significant differences exist in scope, timing and approach. Multinational organizations that experience a data breach may want to take steps to manage the breach across borders.

However, high UK fines after data breaches are not new. The Financial Services Authority (FSA) has already fined financial services organizations double the new ICO maximum after a data breach. It is likely that the ICO and FSA will continue to cooperate on investigations that involve a financial services organization.

The new legislation is likely to raise the bar for those doing business in the UK. Many of the big global breaches over the last few years—such as the TJX and Heartland breaches—have been undertaken by just one crime ring. Other breaches have been committed by sophisticated phishing networks based in Russia and the former Soviet states. This law would not penalize either type of criminal organization, although it could be directed toward imprudent corporations that become "victims"—for example, if a company is negligent and leaves the door open for a phishing attack.

Managing a data breach is often a challenging process. Regulators, both in Europe and the US, have maintained that corporations should have an incident plan in place before they experience a breach, as well as take steps to minimize the risk of a breach happening. The ICO's new powers indicate there is likely to be no respite in regulatory activity in this area in 2010.

For Further Information

If you have any questions this *Alert*, please contact Jonathan P. Armstrong in our London office, Sandra A. Jeskie in our Philadelphia office, any of the members of the Information Technologies and Telecom Practice Group or the attorney in the firm with whom you are regularly in contact.