LexisNexis® Emerging Issues Analysis

Marc J. Lederer on

ICO Issues Its Largest Fine Against a Single Entity for Data Security Breach

2011 Emerging Issues 5859

Click here for more Emerging Issues Analyses related to this Area of Law.

On June 9, 2011, the UK's data privacy regulator, the Information Commissioner's Office (the "ICO"), imposed its biggest fine to date against a single data controller[1] for breaching the UK's Data Protection Act of 1998 (the "Data Protection Act"). The ICO served Surrey County Council ("Surrey") with a monetary penalty of £120,000 for violations of the Data Protection Act that arose out of three separate incidents in which emails containing sensitive personal data[2] were sent to the wrong recipients.[3]

Data Breach Incidents. The first incident occurred on May 17, 2010, and was the most significant of the three breaches. A staff member of Surrey emailed an Excel file containing Sensitive Personal Data[4] of 241 individuals to the wrong group email address, which contained the email addresses of 361 transportation companies. The ICO noted that because the email was not encrypted or password protected, it had the potential to be viewed by a considerable number of unauthorized persons. The ICO also noted that the Surrey staff member who inadvertently sent the subject email had expressed concern, indicating that she was uncomfortable with her assigned task as she had limited experience with computers, had not attended all appropriate IT training and was unfamiliar with Excel. When Surrey discovered the error, it attempted to recall the email and prevent further dissemination of the Sensitive Personal Data, but was

---

1. "Data Controller" under the UK Data Protection Act of 1998 means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed; *The Data Protection Act of 1998, 1998 CHAPTER 29.*

2. "Personal Data" under the Data Protection Act means data that relate to a living individual who can be identified:

   (a) from those data, or

   (b) from those data and other information that is in the possession of, or is likely to come into the possession of, the Data Controller, and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

   "Sensitive Personal Data" under the Data Protection Act includes data concerning an individual's physical or mental health or condition.

3. http://www.ico.gov.uk/~/media/documents/pressreleases/2011/monetary_penalty_surrey_council_release_20110609.pdf; http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/~/media/documents/library/Data_Protection/Notices/surrey_county_council_monetary_penalty_notice.ashx.

4. The Sensitive Personal Data contained in this email related to individuals' physical and mental health.

unable to conclude that all recipients had destroyed such information. Surrey notified the affected individuals (or their representatives) of the breach and reported the incident to the ICO. Within days following this breach, Surrey drafted a safeguarding action plan that included a reminder to management to provide IT training and guidance to employees.

The second incident occurred on June 22, 2010, and was similar in nature to the first incident in that the confidential Personal Data of a number of individuals was mistakenly emailed, this time to over one hundred unintended recipients. Similar remedial action was taken by Surrey following this breach.

Between the time of the second and third security breaches, on September 6, 2010, Surrey issued a report that recommended, amongst other things, that:

1) Specific training be implemented for certain officers;

2) Employees' work activities be included with their job descriptions on relevant documents;

3) A naming convention be established for global email distribution list that would lead to less mistakes; and

4) A technical solution that would warn a staff member when an email or document marked "Protected" or "Restricted" is about to be emailed to an external email address be investigated.

In addition, Surrey carried out an audit of its email security in November 2010, which resulted in a report that recommended, amongst other things, that certain emails containing sensitive information be encrypted. However, the majority of the recommendations made in the September report and the November audit report were not implemented until February 8, 2011 (subsequent to the third security breach).

The third incident occurred on January 21, 2011, and likewise resulted in an individual's health information being sent to the wrong recipient, in this case to an internal group email address. Surrey once again took remedial action as it did in the first two incidents and reported this third breach to the ICO.

ICO Enforcement. The ICO has the authority under the Data Protection Act to levy monetary penalties on a Data Controller not to exceed £500,000, if it is satisfied that:

1) there has been a series of contraventions of the Data Protection Act that were of a kind likely to cause substantial damage or distress; and

2) such contraventions were deliberate; or

3) the Data Controller knew or ought to have known that there was a risk that a contravention would occur, of a kind likely to cause substantial damage or distress, and failed to take reasonable steps to prevent the contravention.

In this case, the ICO found that monetary penalties should be imposed upon Surrey for violating the Data Protection Act because Surrey failed to have the appropriate technical and organizational security measures (training, file naming conventions, email encryption) in place by the time the first security breach had occurred. In addition, the ICO determined that substantial distress was caused due in large part to the number of individuals that were affected, the number of inadvertent recipients, the sensitivity of the information involved, the vulnerability of the individuals affected (individuals receiving day care) and the risk of possible further dissemination of that information. Additionally, the ICO concluded that Surrey ought to have known of the risk and the distress that could result from not taking reasonable steps to prevent a breach from occurring. The ICO came to that conclusion because some of Surrey's employees were used to dealing with Sensitive Personal Data and should have realized the danger in using drop-down boxes to select email recipients for such Sensitive Personal Data. Furthermore, the fact that three separate security breach incidents had occurred served as a factor in determining monetary penalties in this case.

In reaching the decision to impose a monetary penalty of £120,000 upon Surrey, the ICO also cited mitigating factors and other considerations, including:

1) the remedial measures taken by Surrey;

2) the belief that the Sensitive Personal Data has not been further disseminated;

3) that the subject email and attachment were protectively marked, and the sensitivity of the email contents was clear on the face of the email;

4) that the Excel spreadsheet did not contain more information than was necessary to complete the task;

5) confirmation that 213 of the transportation companies that were inadvertently sent the subject email for the first incident either did not receive it or deleted it;

6) that Surrey voluntarily reported the breach to the ICO;

7) that Surrey compiled detailed investigation reports following the security breach;

8) that affected individuals (or their representatives) were notified of the breach; and

9) the fact that payment of the monetary penalty will not result in undue hardship upon Surrey because of its financial resources.

Finally, the ICO noted that following these security breach incidents, Surrey has improved its policies by developing an early warning system that alerts staff when Sensitive Personal Data is being sent to an external email address, as well as improving staff training and ensuring that any group email addresses are clearly identifiable.

The ICO's Warning to Others. By imposing the monetary penalty in this case, the ICO also wanted to send a message that Data Controllers must have appropriate and effective security measures in place in order to comply with the Data Protection Act. As ICO Commissioner Christopher Graham stated: "Any organisation handling sensitive information must have appropriate levels of security in place. Surrey County Council has paid the price for their failings and this case should act as a warning to others that lax data protection practices will not be tolerated."

Accordingly, whenever a data privacy regulator like the ICO imposes a penalty upon an organization, it is always recommended that companies conduct a review of their own policies and procedures to ensure that they are in compliance with any applicable privacy and data security laws or regulations.

Click here for more Emerging Issues Analyses related to this Area of Law.

Marc J. Lederer on
ICO Issues Its Largest Fine Against a Single Entity for Data Security Breach

About the Author. Marc J. Lederer is a privacy law attorney at Willkie Farr and Gallagher LLP in New York, NY. He regularly counsels clients on privacy and data security issues. Mr. Lederer advises financial institutions as to compliance with the numerous federal, state, and international privacy and data security laws. Mr. Lederer can be reached by phone at 212-728-8624 or by email at mlederer@willkie.com.