Client Alert: Hilton Settles US data breach action

Date : November 1, 2017

Yesterday the New York Attorney-General Eric T. Schneiderman announced a $700,000 settlement with Hilton hotels after two data breaches in 2015 exposed over 350,000 credit card numbers in two separate breaches.

Whilst in the US there are no general data protection laws equivalent to those in Europe the investigation was based on Hilton's failure to notify the victims in time and their failure to maintain reasonable data security despite the promises they made in their privacy policy.

Most US states have data breach laws in place which require a company to notify victims after a breach. In some respects these obligations are similar to those which will apply across Europe from 25th May 2018 when new European data protection law, the General Data Protection regulation (GDPR) enters into force. There is more about GDPR in our GDPR FAQs here www.bit.ly/gdprfaq.

According to the New York A-G Hilton also made a misleading statement in their privacy statement on their website when they said that Hilton "*will take reasonable measures to: (1) protect personal information from unauthorized access, disclosure, alteration or destruction and (ii) keep personal information accurate and up-to-date as appropriate*." Hilton also represented that it would keep its customer's personal information "*secure*."

In announcing the settlement Schneiderman said "*Businesses have a duty to notify consumers in the event of a breach and protect their personal information as securely as possible, Lax security practices like those we uncovered at Hilton put New Yorkers' credit card information and other personal data at serious risk. My office will continue to hold businesses accountable for protecting their customers' personal information."*

This isn't the first action like this in New York. For example in 2003 Victoria's Secret reached a somewhat similar settlement with the then New York A-G after a website technology flaw was found.

In addition to paying $700,000 Hilton have agreed to provide immediate notice to those consumers affected, maintain a comprehensive information security program, and conduct data security assessments.

Does this touch Europe?

Schneiderman said in announcing the settlement that one of the compromised servers was in the UK. It is important to remember that the jurisdiction provisions also change under GDPR which would give EU regulators even more reach to deal with data breaches affecting the EU. Currently, under the UK Data Protection Act 1998 (DPA 1998) UK law will apply if the data controller "*uses equipment in the United Kingdom for processing the data otherwise than for the purposes of transit through the United Kingdom*." That may well be the case here. If so it will be interesting to see if the Information Commissioner's Office does take action. Under DPA 1998 the maximum fine for breach is currently £500,000. Under GDPR the potential fine could be higher – in Hilton's case based on its 2016 turnover the maximum fine could be around $466m although it is fair to say that the ICO has not currently levied the maximum fine nor would a fine of $466m be likely under GDPR in a case like this.

Additionally it may well be that the New York settlement opens up the possibility of civil actions from those affected. We have talked about the likelihood of civil actions after data protection breaches before, for example in our alert last year on the Google v. Vidal – Hall case http://www.corderycompliance.com/vidal-hall-data-protection-class-action-appeal-settled/. It could be that the consequent civil actions and reputational damage may be more damaging than any monetary penalty from the ICO. Additionally given the move to GDPR any organisation dealing with Hilton – for example entering into preferred supplier arrangements for rooms for its employees – will have to increase its pre-contract due diligence.

Lessons learnt

Organisations with operations in the US may wish to take advice from appropriately qualified US counsel on their

response. From a European point of view some of the lessons to be learnt include:

1. Organisations need to have proper processes and technology in place for detecting, assessing and reporting breaches. There's more information on what we think this should include here: http://www.corderycompliance.com/dealing-with-a-breach/
2. Rehearsing for a data breach is of critical importance. Under GDPR the time to report a breach may be as little as 72 hours. Organisations will need to practice beforehand to have a chance of reporting in time. Cordery's Data Breach Academy in January might be useful in helping organisations prepare: http://www.corderycompliance.com/cordery-data-breach-academy/
3. Review you privacy policy. Too often we see organisations making unrealistic claims in their privacy policies about data security. Even the best run organisations cannot guarantee that the internet is secure. Their privacy policies should not suggest they can.
4. Get up to speed with GDPR. Cordery's GDPR Navigator has a whole host of data protection resources to help deal with data breaches including a detailed guidance note on the security aspects of GDPR, a short film describing a company's security obligations and giving tips on how to deal with a data breach, a template data breach report, a specimen data breach log and a data breach procedure. There are more details of GDPR Navigator here www.bit.ly/gdprnav.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com