Client Alert: Blackbaud Revisited

Date : January 12, 2022

Introduction

In July 2020 we looked at one of the biggest ransomware attacks that year involving Blackbaud, one of the world's largest providers of CRM systems for the higher education, healthcare and not for profit sectors. As litigation rumbles on after the attack in the US and the UK we thought it might be worth taking a look almost a year and a half later at the lasting effects of the attack. The consequences are still being felt for Blackbaud and for its many customers including some of the UK's largest charities and universities.

Some technical terms are used in this note which are explained at www.bit.ly/gdprwords. There is a general background to ransomware here https://bit.ly/cvransom.

What happened?

Blackbaud was a service provider to a large number of institutions around the world. In recent years it had acquired a number of different organisations including the funding platform JustGiving. It described itself at the time of the attack as "*the world's leading cloud software company powering social good*."

According to Blackbaud, it discovered in May 2020 that it had had a ransomware attack on its systems. It said that some data was compromised and a number of universities and other organisations using its services had been affected. Apparently Blackbaud waited until 16 July 2020 to tell its customers. Our note in July gave more background on the attack and the organisations affected. You can read that note here https://bit.ly/blackcrack.

What are regulators doing now?

We said in July 2020 that the UK data protection authority, the Information Commissioner's Office (ICO) was investigating the attack. It seems that this investigation is still ongoing. Blackbaud has said that it is also facing investigations from DPAs in Australia, Canada, Ireland and Spain.

In the US Blackbaud has said that it has received a subpoena from 44 State Attorneys General and the District of Columbia, and information requests from the US Federal Trade Commission, the US Securities and Exchange Commission, and the US Department of Health and Human Services.

Blackbaud maintains that it stopped the attack before personal data was shared publicly. At least one customer has however said that it believes that its data was exposed.

What about class actions?

As we said in our July 2020 note threats of litigation were always inevitable. We've seen many ransomware attacks be followed by threats of litigation, sometimes less than 48 hours after details of the attack become public. It is far from clear that cases like this will always succeed, especially when there's no exfiltration of data and little or no damage. In the UK, Germany and some other European countries there have been cases in the last few months which will help potential defendants (including the Lloyd case here https://bit.ly/lloydsc and the Johnson case here https://bit.ly/eastlight2) but from our experience that does not stop claims like this being threatened.

In the UK there is threatened group action litigation against a number of Blackbaud customers including The Labour Party and The National Trust. One law firm has said it is investigating claims against 9 UK universities.

There is also a class action in the US and Blackbaud was recently criticised at a hearing in that litigation in South Carolina for not providing the plaintiffs with sufficient information about the attack.

What can organisations do to avoid this happening to them?

As we said in our alert in March 2020 (here www.bit.ly/cvransom) ransomware is on the rise and criminals are increasing the number and sophistication of attacks. There has been no let up in the size and scale of ransomware attacks – in fact according to the BlackFog ransomware report December 2021 was the busiest month. Organisations need to strengthen their defences. That will include:

1. Doing proper due diligence on the Data Processors you use. As part of the due diligence exercise you should make sure that the provider has adequate technical and organisational measures in place.
2. Looking in detail at contracts with vendors and other third parties. You will need to look carefully at emphasising a Data Processor's obligations to let you know immediately if they suspect a possible breach. In our view audit rights are also important – too often Data Controllers are vague about cause and effect and it can take the exercise of audit rights to get proper information.
3. The contract should also back the Data Processor's obligations with proper penalties when things go wrong. All too often we see Data Controllers agreeing to contracts which cap liability at unrealistically low levels. That is unlikely to be a defensible position under GDPR.
4. You may also want to consider your position on ransomware payments and agree a strategy in advance. We have a more detailed note looking at the 'To Pay or Not to Pay' considerations for ransomware here https://bit.ly/ransompay. It appears that Blackbaud faces further litigation in the US for paying a ransom.
5. Preparing for a breach. Breaches are inevitable so preparation is key. This might include having good lawyers on standby since we know that the initial hours after a breach are crucial in successfully defending claims. This is also likely to include rehearsing a breach for example with a Cordery Data Breach Academy (see https://www.corderycompliance.com/cordery-data-breach-academy-2-2/).
6. Finally it is worth remembering that you're unlikely to be able to insure this risk away – insurers are tightening up on coverage where ransomware is involved.

Further information

You can read the BlackFog ransomware report here https://bit.ly/bfreport2.

For more information on how we handle data breaches see our film here https://www.corderycompliance.com/dealing-with-a-data-breach/ and our note here https://www.corderycompliance.com/dealing-with-a-breach/.

For a more detailed discussion on ransomware you can listen to Jonathan Armstrong talking with Richard Levick here https://www.corderycompliance.com/ransomware-in-house-warrior/ and watch Jonathan talking to Don Smith of Secureworks here https://www.corderycompliance.com/cordery-head-to-head-don-smith-ransomware/.

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