PRIVACY BREACHES IN M&A DEALS AND THE IMPORTANCE OF DATA SECURITY DILIGENCE

Posted on April 3, 2023

Categories: Insights, Publications

In 2006, British mathematician Clive Humby famously declared "data is the new oil." Indeed, data is becoming increasingly important in a growing number of industries. That is why, when deciding whether to proceed with an M&A transaction, it is imperative to assess the privacy and data security controls of the target company.

As we have written about in the past, numerous privacy issues can negatively impact an M&A transaction. A company's failure to comply with CASL[1] can potentially lead to serious fines. A company's mismanagement of consent can render large amounts of personal information virtually useless. With overhauls to Canada's privacy regime (including serious penalties) both in progress and on the way, bringing a company's privacy management program up to standard is only becoming more costly.

However, there may be no privacy issue more significant to a transaction than the **threat of a data breach**. Data breaches can result in regulatory notification and disclosure obligations, class actions, harms to reputation, and regulatory penalties. Even where personal information is not concerned, data breaches can expose intellectual property or other confidential information, or disrupt a company's operations.

In this bulletin, we focus on the importance of data security diligence, tips for the diligence process, and mitigation strategies for companies that have identified risks and wish to proceed with the deal. We also discuss the need to assess and quickly remediate any flaws in a target company's data security program following a transaction.

Recent Examples of Data Breaches Affecting Corporate Transactions

Data breaches discovered both during and after a corporate transaction can have significant ramifications on a deal and the companies involved.

For example, in 2016, a pair of data breaches that were identified prior to finalizing the acquisition of Yahoo by Verizon caused the sellers to lower the purchase price by $350 million USD.[2]

Additionally, in *PIPEDA Findings #2022-005*, the Office of the Privacy Commissioner of Canada (OPC) investigated the purchaser for failure to mitigate a data breach that had already been deployed on the target

company's systems prior to closing. In 2014, a cyber attacker successfully infiltrated and installed malware on the target company's systems. At the time of the transaction, in 2016, neither the purchaser nor the target were aware that the target's internal database was infected. The data breach was only discovered in 2018, at which point the attackers had already downloaded up to 339 million records from the database.

After discovering the breach, the purchaser was investigated by both the UK Information Commissioner's Office (ICO) and the Office of the Privacy Commissioner of Canada (OPC). Following its investigation, the ICO announced its intention to fine the purchaser €99 million (the fine was later reduced to €18.4 million). The ICO's investigation found that the purchaser failed to undertake sufficient due diligence when it bought the target, and should have done more to secure its systems.[3]

The OPC issued its investigation report in September 2022, largely agreeing with the ICO's findings. In particular, the OPC found that the purchaser could have detected the breach sooner and minimized the effect of the breach if it had: (i) put more comprehensive logging and monitoring measures in place, (ii) adequately applied its multi-factor authentication access controls, and (iii) put stronger accountability measures in place to make sure its security safeguards are assessed and updated on an ongoing basis.

Data Security Diligence

To mitigate against the risks associated with data breaches, purchasers should incorporate a data security assessment into their due diligence strategy, especially where data is an important part of the transaction or sensitive personal information is regularly collected by the target. In particular, purchasers should consider requesting the following things from target companies in the due diligence process (without limitation):

- Copies of data security policies, including but not limited to physical and technical security plans, data backup procedures, and breach response plans;
- Information about the types of personal information collected, and whether the company has retention and destruction policies in place;
- Information about personnel management, including whether the company conducts background checks for employees, requires employees to sign confidentiality statements, or conducts cybersecurity training;
- Information respecting how the company handles third parties, including assessments of the data security posture of service providers or related companies that handle data on the target's behalf;
- Information about privacy and cybersecurity audits (both internal and external), including how often they are conducted and copies of recent reports;
- Information about past data breaches (including remediation steps taken); and
- Copies of cybersecurity insurance policies, if any, and information on past claims made under such

policies.

Where the volume or sensitivity of target company data is high, purchasers should consider engaging information technology experts (either internal or external) in order to evaluate the target company's data security controls.

It is important to obtain experienced outside counsel to determine which privacy and data security issues constitute red flags, and which ones may simply impact the valuation of the target company.

Mitigation Strategies

So you've discovered a serious data security issue with the target company. Should you walk away from the deal altogether?

In most cases, subject to a purchaser's risk tolerance, flaws in a business's data security program are not fatal to the deal. There are several options a purchaser may wish to consider to mitigate the risks. For example, a purchaser may:

i. negotiate an indemnity for any penalties or litigation costs associated with data breaches that occurred prior to, or within a reasonable period after closing;
ii. negotiate a price reduction to account for the risk of a data security incident;
iii. negotiate a holdback or escrow; or
iv. negotiate a requirement in the purchase agreement that the target remediate their data security program prior to or immediately after closing.

Some purchasers may look to obtain representations and warranties insurance (RWI) to protect against data security risks. However, RWI is not always a viable option to address data security issues, particularly when there is a known issue. Underwriters have recognized the significant financial consequences of a data breach, and often limit, or completely exclude costs of managing data security issues from their RWI policy.

Where an RWI policy does include data security coverage, underwriters now require the target company to meet minimum security controls, as determined by the purchaser's fulsome due diligence review.

Takeaways

- Acquiring a company can expose a purchaser to liability for past data breaches;
- Malware can sit undetected in a company's system for a long time;
- In the due diligence stage of a corporate transaction, appropriate external parties (including experienced legal counsel and IT security professionals, as needed) should be brought in to ensure the target's data security systems are up to standard, considering the volume and sensitivity of the data in the company's

possession or control;
- Risks to a deal may be mitigated through various negotiation tactics, or through RWI policies (but such policies cannot always be relied upon);
- Post-closing, it is vital to account for all data in the company's possession and ensure that data is protected.

[1] *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23, commonly referred to as "Canada's Anti-Spam Law" or "CASL".
[2] Wall Street Journal, *Why Verizon Decided to Stick With Yahoo Deal After Big Data Breaches* (July 2017), available online. The end purchase price was $4.48 billion USD.
[3] UK ICO, Case ref: COM0804337 (October 2020), available online.

by Robbie Grant, Mitch Koczerginski, Adriana Rudensky and Christopher J. Garrah

A Cautionary Note