SCENARIO 2

Infinite Airlines is a major international airline operating out of several jurisdictions but with its home in the United Kingdom. The airline's Australian operations are based out of Sydney Airport. The Chief Technical Officer of the company, Meera, was recently informed by her cyber resilience team members of a large-scale cyber-attack which resulted in a massive data breach. Although they are still assessing the scale of the damage they are estimating a leak of the bank details of approximately 500,000 customers. Panicked by the potential fallout and scandal that will inevitably flow from this criminal attack, the Board of Directors of Infinite Airlines immediately contacts their go-to law firm AdaptingLaw and, based on their advice, the specialist Cyber Security consultancy, CleaningUpYourCyberMess. AdaptingLaw is a large international firm with its home office in Sydney. The firm offers a broad range of services with clients from both the private and public sectors and is well-known to provide ongoing advice to the Australian Federal Government. However, the firm only has an emerging practice in Cyber Security with one partner, Louise, and her small team covering this area.

Within 48 hours of the discovery of the attack, CleaningUpYourCyberMess completes the initial analysis of the event in order to prioritise a patching of the vulnerability. During this analysis, the CleaningUpYourCyberMess emergency response team discovers that the problem stemmed from what appears to be a systemic security vulnerability in the infrastructure provided by the Cloud computing service provider, CloudedCapacity – a large multinational corporation headquartered in Silicon Valley. On the advice of CleaningUpYourCyberMess, Infinite Airlines informs CloudedCapacity who immediately takes action.

Infinite Airlines has been using the services of CloudedCapacity for the last 5 years when they replaced the corporate IT systems at its premises in London with the more dynamic leased infrastructure. Infinite Airlines informs Louise and her team at AdaptingLaw of the cause of the breach and asks her to review its agreement with CloudedCapacity and for her advice regarding contractual liability and any potential regulatory risk. Given the scale of the matter, Louise involves AdaptingLaw's managing partner Eva given her expertise in commercial litigation. When describing the events Louise is shocked to learn that AdaptingLaw also uses the services of CloudedCapacity. The firm immediately also engages the services of CleaningUpYourCyberMess and discovers their exposure to the same security flaw. This vulnerability has caused the leak of detailed client files. The firm is horrified by the breach of client privilege and starts preparing to blame CloudedCapacity. However, before AdaptingLaw manages to even inform CloudedCapacity of the breach, the Cloud Service provider issues a public statement detailing the effects of the breach stating that all clients had been exposed to the same fault. In their public statement, CloudedCapacity states that the security vulnerability had been exposed by what appears to be a sophisticated attack.

The cross-jurisdictional nature of the events clearly complicates matters and when reviewing the respective contracts between CloudedCapacity and AdaptingLaw and

Infinite Airlines, Louise and Eva notice a choice of jurisdiction and choice of law clause indicating that Californian law applies. They wonder about the intersection between this contractual clauses and inter alia national cyber security and data privacy legislation. This matter is further complicated by the fact that the firm and the client are based out of different jurisdictions. In addition, from its public statements CloudedCapacity appears to be washing its hands of any responsibility pointing to a clause within its standard contractual agreement absolving it of liability stemming from a sophisticated attack provided it had maintained 'state of the art' security.

AdaptingLaw is scrambling to figure out their legal liability let alone that of their client, and any means of recourse open to them. Globally companies are also scrambling to assess their situation and regulatory authorities across various jurisdictions (e.g. Data Protection Authorities) have made public statements indicating that they have investigations under way.