My chosen case was Court Ventures (Experian).

**What types of data were affected?**

Social Security numbers, birth dates, physical addresses (current and previous), mobile numbers, and email addresses. In other cases he was able to obtain and sell credit card numbers and the expiration dates of those cards.

**What happened?**

An individual named Hieu Minh Ngo, pretended to be a private investigator in Singapore and then contracted with a company called Court Ventures. Court Ventures had a contract with a company called US Info Search, which allowed customers of Court Ventures to get data from US Info Search, and vice versa.

Consequently, Ngo was able to exploit this relationship and sell data available on the US Info Search database to his clients, who intended to use it for fraudulent purposes.

**Who was responsible?**

A single person- Hieu Minh Ngo.

**Were any escalation(s) stopped - how?**

The article doesn't say.

**Was the Business Continuity Plan instigated?**

No

**Was the ICO notified?**

No

**Were affected individuals notified?**

No

**What were the social, legal and ethical implications of the decisions made?**

This was an interesting case study because it happened before personal data became valued and treated as something which needs the utmost protection. From today's perspective, the response of Court Ventures was lackluster and no concern was given to the affected individuals' data after the discovery of the breach. The most severe implications were on an ethical level because affected individuals were not informed of the breach, increasing the risk that they could be defrauded. However, no real legal implications occurred from the poor response to data compromise, due to the lack of regulations and governing bodies at the time.

**If you had been the ISM for the organisation you selected what mitigations would you have put in place to stop any reoccurrences?**

The root cause of the incident here is that Court Ventures failed to do due diligence on Ngo, allowing him to obtain access to such sensitive information. The first step is therefore to introduce more thorough processes for potential clients (especially international ones).

**Bibliography**

Krebs, B. (2014) Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records. Available from: <https://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/> [Accessed 10 February 2022].

Goss, G. (2015) Vietnamese man gets 13 years for massive ID theft scheme. Available from: <https://www.computerworld.com/article/2948295/vietnamese-man-gets-13-years-for-massive-id-theft-scheme.html> [Accessed 10 February 2022].