GDPR Violation Case Study: Ticketmaster UK

Kate Nelson, Mason Zhang, and Amanda Lee

1. Abstraction:

Data breaches have been an increasingly common phenomenon in recent times. As a product of our digital economy, consumers enter their personal information into websites several times a day. At the same time, companies have been reluctant to invest in strong cybersecurity, viewing it as an unnecessary expense. Even if a company's codebase is secure, they have to ensure that all third party tools and software are as well. Adversarial actors have evolved to exploit companies' lax security practices to obtain vast amounts of personal data, including credit card data. The GDPR outlines a company's responsibilities in the event of a data breach and provides a framework towards punishing companies deemed negligent in securing their users' data.

2. Background:

The three major parties involved are Ticketmaster UK, Inbenta Technologies, and the Information Commissioner's Office. Ticketmaster UK is a ticket sales and distribution company used by venues and artists to manage their events. Ticketmaster generates revenue through service and processing fees levied on each ticket sold. In 2018, their sales reached 500 million tickets across 400,000 events. Inbenta Technologies provides various services rooted in artificial intelligence technology, including several "conversational AI" products, one of which was employed by Ticketmaster. The Information Commissioner's Office is the United Kingdom's independent data protection regulator. The authority was created in 1984, and it is funded by the Department for Digital, Culture, Media, and Sport of the UK government. Its role is to promote data privacy for users and transparency on the part of data-handling entities.

3. Violation Detail:

The Information Commissioner's Office found Ticketmaster UK guilty of failing to keep customers' personal data secure, resulting in a security leak that compromised the data of 9.4 million users and a fine of $1.25 million.

3.1 Security Leak

Ticketmaster, the data controller, employed Inbenta Technologies's chatbot service as the data processor. Ticketmaster included a chatbot on its payments page. The code behind the chatbot was hosted by Inbenta, and the attacker targeted the Ibenta servers, inserting malicious code that recorded information inputted into the payments form by platform users. The attacker achieved this through an event listener that intercepted form post requests.

On April 6, 2018, 50 customers of Monzo Bank reported fraudulent transactions. Six days later, Ticketmaster representatives met with Monzo Bank employees. Monzo Bank discovered that one of the users entered an

incorrect card expiration date when using Ticketmaster's service. That same incorrect date was then used again for a fraudulent transaction — a "smoking gun" (ICO). As early as February 2018, Inbenta was aware of a potential security issue with its product. It was not until June 23 that Ticketmaster issued a formal notice of the security breach. Ticketmaster disabled the chatbot on June 23, and in its communication to regulatory bodies, claimed that the leak was uncovered on June 22.

The ICO investigation ultimately concluded that Ticketmaster had failed to "assess the risks of using a chat-bot on its payment page," "identify and implement appropriate security measures to negate the risks," and "identify the source of suggested fraudulent activity in a timely manner."

3.2 Violated Articles

GDPR's Article 5 of Chapter II defines principles relating to the processing of personal data:

- Article 5 (1): lists the six basic principles that controllers must comply with when processing, including: 1. Personal data shall be: ... (f) processed in a manner that ensures appropriate security of the personal protection damage, using appropriate technical or data, including against unauthorised or unlawful processing and against accidental loss, destruction or organisational measures ('integrity and confidentiality')
- Article 5 (2): makes it clear that the "controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".

GDPR's Chapter IV, Section 2 addresses security of personal data. GDPR's Article 32 states that "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…".

Ticketmaster failed to comply with its obligations under Article 5(1)(f) and Article 32 of the GDPR. It failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using 32 appropriate technical and organisational measures as required by Article S(l) (f) and Article 32 GDPR.

3.3 Consequences

Ticketmaster was negligent in the security surrounding its payments page chat-bot, resulting in a cyberattack that affected 9.4 million data subjects, including 60 thousand individual payment card details. There were nearly 1000 complaints of financial loss, and the company was ultimately fined a penalty of $1.25 million (ICO).

3.4 Prevention

Additional precautions should always be taken when contracting a third party service, especially if that service is employed in proximity to sensitive data. ICO found that, at the time of the breach in 2018, Ticketmaster had last vetted Ibenta's cybersecurity posture in 2013, which the

ICO said was insufficiently recent given the pace with which cybersecurity threats evolve. Ticketmaster should have conducted more stringent reviews of the service that they were using on their payments page. For instance, in the contract with Inbenta, Ticketmaster could have required regular security reviews for more visibility, or an external audit that would have informed the company of how secure the service is and how much trust to afford it. Furthermore, Ticketmaster could have acted more rapidly after being notified of a potential security issue.

4. Discussion

The case could've been handled better in a couple different ways. Firstly, during the investigation, the ICO found concrete evidence that Ticketmaster's infrastructure had been compromised in February. Despite these findings, the ICO imposed a fine that only covered the period from May onwards. I understand that GDPR only went into effect in May, but Ticketmaster attempted to take advantage of this limitation to avoid admitting liability for the breach in the first place, which is problematic. Additionally, the First-tier tribunal approving Ticketmaster's application to stay means that the process will remain unfinished until 2023, five years after the breach happened. Supposedly, it was approved because the tribunal wanted to wait for the judgements of other High Court proceedings to be made, but this seems like a pretty long delay. With such a big case, could they not move forward with a ruling and have this case establish a precedent for future rulings? This case was incredibly important because the breach was due to malicious code being injected into a third party software that Ticketmaster was using on their website. Ticketmaster hoped to absolve themselves of responsibility and instead blame the third party, but the ICO was unreceptive. This established that companies must implement their own security controls and diligently check any third party software that they may use. Companies must also be aware of up and coming attack vectors, as Ticketmaster's argument that ICO was engaging hindsight bias was not well received.

References

Home | ICO. Information Commissioner's Office. (n.d.). Retrieved September 21, 2021, from https://ico.org.uk/.

GDPR Official Legal Text. General Data Protection Regulation (GDPR). (n.d.). Retrieved September 23, 2021, from https://gdpr-info.eu/.

ICO fines Ticketmaster UK LIMITED £1.25million for failing to Protect customers' payment details. ICO. (n.d.). Retrieved September 23, 2021, from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/ico-fines-ticketmaster-uk-limited-125million-for-failing-to-protect-customers-payment-details/.

Inbenta Technologies Homepage. Inbenta. (2021, June 7). Retrieved September 23, 2021, from https://www.inbenta.com/en/.

Page, C. (2020, November 13). *Ticketmaster hit WITH £1.25 Million GDPR fine OVER 2018 data breach*. Forbes. Retrieved September 23, 2021, from https://www.forbes.com/sites/carlypage/2020/11/13/ticketmaster-hit-with-125-million-gdpr-fine-over-2018-data-breach/.

Ticketmaster UK Ltd MPN. ICO. (2020, November 13). Retrieved September 23, 2021, from https://ico.org.uk/media/action-weve-taken/2618609/ticketmaster-uk-limited-mpn.pdf.

Ticketmaster. Ticketmaster: Buy Verified Tickets. (n.d.). Retrieved September 21, 2021, from https://www.ticketmaster.com/.