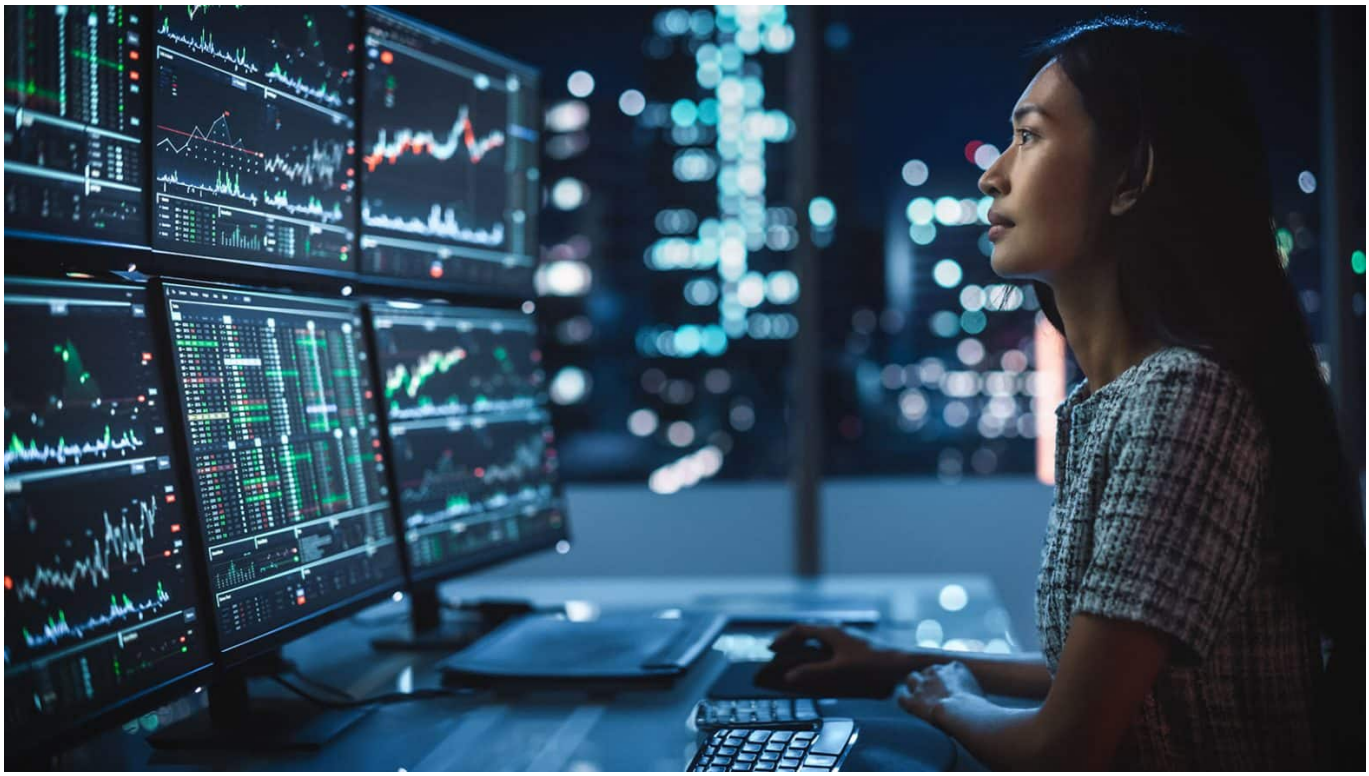
Check your chat bots: lessons from Ticketmaster's £1.25m fine



In November, Ticketmaster was fined £1.25 million by the ICO for failing to appropriately secure customer data. Similar levels of penalties have also been levied against the likes of Marriott International and British Airways. The amount of these fines reflects the size and turnover of these particular businesses, but also the willingness of the ICO to hand out the toughest penalties for serious breaches of data protection laws. This underlines that no business can afford not to take data security seriously.

What happened?

Ticketmaster had introduced a third party chat bot function onto its website, crucially including it on its payment page. According to the third party provider Inbenta Technologies Inc., the chat bot had not been intended for use on the customer payments page due to the security risk posed.

Card issuers informed Ticketmaster of fraudulent activity experienced by cardholders who had all used the Ticketmaster website. 60,000 Barclays customers were victims of fraud, and Monzo had to replace 6,000 payment cards due to fraud. Investigations carried out by Ticketmaster revealed cyber attackers had used code inserted into the chat bot Javascript to collect confidential customer details, including payment card information.

How could this have been prevented?

In the ICO's Penalty Notice, it outlined that Ticketmaster failed to recognise the widely known risk of implementing third-party JavaScripts into the chat bot function. Ticketmaster could have implemented technical

measures to mitigate this risk, such as using sub-resource integrity, or could have not used the chat bot function at all.

The increased likelihood and severity of an attack should have been recognised by Ticketmaster, with financial data attacks more likely through a third party supply chain where security measures may be less secure. Ticketmaster should have ensured an acceptable level of security was maintained, and tested the security measures between the chat bot and its payments page. Ultimately, this function should not have been included on its payment page at all.

Ticketmaster has also been criticised for its delayed response after being alerted by banks of the potential fraud. The issue with the chat bot was not detected quickly enough, and Ticketmaster did not begin monitoring network traffic through the online payment page until nine weeks after the alert.

Top Tips for businesses

- ensure tight security controls around payment card details;
- do a formal risk assessment before deploying new tech or using existing tech with different data sets;
- ensure data security policies are up to date and procedures followed, with staff properly trained to spot and respond to risks and breaches; and
- check third party data processing arrangements comply with the GDPR and provide suitable contractual protections to you in the event of problems.

How we can help

For information and advice in relation to data protection, please contact Elliot Fry at elliot.fry@cripps.co.uk.

Written by

Elliot Fry

Managing Associate