Related Articles

reflectiz.com/ico-fines-ticketmaster-uk-1-25-million-for-security-failures-a-lesson-to-be-learned/

November 26, 2020

The ICO Fines Ticketmaster UK £1.25 Million for Security Failures: A Lesson to be Learned

Ticketmaster UK, a leading ticketing company and part of Ticketmaster, has been fined £ 1.25 million by the Information Commissioner's Office (ICO) as it failed to protect customer data during

the infamous February 2018 data breach. The company is still not taking ownership of the breach, caused by a third-party application exploit! So what really went down in 2018 and who is responsible? Let's break it down.

Although Ticketmaster UK is not an eCommerce entity, online transactions are happening everywhere and opening up millions of attack options for hackers. This development has come at a very crucial time, as hundreds of millions of people are expected to shop online ahead of the upcoming holiday season.

ICO: "Ticketmaster Failed to Implement a Layered Security Approach"

Inbenta Technologies is a leading figure in this story. As mentioned earlier, Ticketmaster UK implemented Inbenta's chat-bot code in its ecosystem.

Since the attacks began in February of 2018 and continued till June 2018, when the rouge Inbenta plugin was finally removed, the case was unclear and so were the financial and legal implications. But as we all know now, it has been decided by the ICO to issue the fine in compliance with the new 2018 GDPR rules.

Ticketmaster was found to have directly violated the Article 5(1)(f) and 32 requirements of the General Data Protection Regulation (GDPR)
ICO representatives state that Ticketmaster UK should have done more to protect its users and that it single-handedly put millions of people at risk as it failed to adopt a layered approach to security, which included the failure to meet the exact PCI-DSS requirements at that time.

James Dipple-Johnstone, Deputy Commissioner said:

> "When customers handed over their personal details, they expected Ticketmaster to look after them. But they did not.
>
> "Ticketmaster should have done more to reduce the risk of a cyber-attack. Its failure to do so meant that millions of people in the UK and Europe were exposed to potential fraud.
>
> "The £1.25million fine we've issued today will send a message to other organisations that looking after their customers' personal details safely should be at the top of their agenda."

Source: ICO Blog

In the meanwhile, Ticketmaster is claiming that Inbenta Technologies software compromised its security measures and plans to appeal against the fine. Inbenta, the vendor that provided Ticketmaster with the chat-bot plugin, said that Ticketmaster misused the code which led to exposure risk in the first place.

With both sides looking at a long legal tussle, who is really responsible for the data breach? Is Ticketmaster right in appealing the latest ICO ruling?

Nevertheless, it's clear now that the regulators refer to Ticketmaster as fully accountable for the 2018 incident. No matter how you look at it, it is also clear that any online business, regardless of the sector, must do everything it can to monitor its third-party apps and avoid security risks.

The Third-Party Inbenta Chat-Bot Plugin That Went Rogue

Even though the third-party provider Inbenta accepts that its JavaScript code caused the problem in the Ticketmaster online payment system, it claims that the ticketing company should not have added the code directly to the pages. In other words, Inbenta is pleading innocent in the aforementioned case.

Being placed on the checkout pages without any security measure (as claimed by the third-party vendor Ibenta Technologies), the code had access to sensitive customer information. This was targeted by attackers, who successfully modified the script, executed the breach, and harvested the data.

Fortunately enough, the code was specifically customized to meet Ticketmaster's requirements, therefore no other platforms were compromised.

As mentioned earlier, there was a debate around the fact that the script was stored on Inbenta servers, arguably making it responsible for the breach.

But the ICO put a stop to the speculations by determining that Ticketmaster is to blame, regardless of the direct involvement of Inbenta Technologies.

> ***"The GDPR does not prevent an organisation from implementing third-party scripts. Rather, the GDPR requires that each organisation assess the risks arising in the circumstances of their own implementation and put controls in place to protect the personal data that it processes"***
> *Source: ICO, Information Commissioner's Office, PENALTY NOTICE; Section 6.26, The ICO Ticketmaster UK Ruling.*

Ticketmaster was not the only company to be attacked in 2018. Magecart has been targeting third-party software components in order to obtain access to sensitive information for years. Magecart attacks third-party platforms and replaces their code with their own malicious scripts to harvest personal data.

British Airways is another major Magecart victim. As per the ICO, which issued a $230 million fine on the aviation giant, over 500000 customers' details were exposed due to a GDPR breach. The fine was reduced to $20 million in October 2020. In that case the third-

party app involved was a user-experience solution called Modernizr, which was manipulated to gain unauthorized access to the data.

GDPR: Why is Ticketmaster Accountable for the Third-Party Breach?

There have been many discussions about who is responsible and why Ticketmaster was fined instead of Inbenta, the third-party vendor? But first things first, what is GDPR? It's basically an EU regulation that coordinates data privacy and protection laws within the European Union, but also affects companies doing business in Europe.

How does GDPR describe the data protection process and find the accountable party? It makes a distinction between data controllers and data processors.

Data Controllers – Controllers are businesses or individuals that make decisions about data processing, which essentially makes them in charge of these activities. Although entire companies can be seen as controllers, in reality, only the decision-makers will be subject to GDPR regulations.

Data Processors – Unlike controllers, processors do not make decisions about processing activities and act solely on behalf of controllers. Serving controllers' interests, processors only process the relevant information as instructed and required by controllers, including some daily operations.

If processors act on their own without the controllers' consent or permission, they will be seen as controllers and bear full responsibility for the consequences. Processors can also be both organizations and individuals. Employees of the controller are neither controllers or processors.

The Bottom Line: Companies must implement appropriate security controls to avoid risks created by their third-party application.

The fact is that Inbenta didn't make any controlling or processing decisions without Ticketmaster's permission, nor did it influence any activities.

Hence, the third-party chat-bot vendor is not legally responsible for the 2018 Ticketmaster data breach. Ticketmaster misused its piece of code and thus is fully accountable for the consequences. It failed to correctly use the code and detect the data breach source, while neglecting warning signs from banks.

In this case, Ticketmaster will probably be paying the full sum of the penalty that has been decided upon by the Information Commissioner's Office.

eCommerce websites, online retailers, and online services providers like Ticketmaster UK, now have to take full responsibility for their eco-systems. More emphasis must be placed on third-party applications. In practice, companies are now required to start monitoring their behavior and not just depend on traditional solutions that are becoming increasingly ineffective.

The growing blind-spot of third-party app security is proving to be very costly. Remember, it may be a third-party code, but security – is now your responsibility.

Additional reading and sources:

ICO, Information Commissioner's Office, PENALTY NOTICE *(re Ticketmaster UK). Click here to view the full notice*

The ICO Blog and News section: ICO fines Ticketmaster UK Limited £1.25million for failing to protect customers' payment details.
Click here to read the ICO's blog post