# PENALTY NOTICE

## Section 155, Data protection Act 2018

**Case ref:**
**COM0759008**

**Organisation name and address:**

**Ticketmaster UK Limited,**

**30 St. John Street, London, EC1M 4AY**

**13 November 2020**

## INTRODUCTION & SUMMARY

1.1 This Penalty Notice is given to Ticketmaster (UK) Limited ("**Ticketmaster**") pursuant to section 155 and Schedule 16 of the Data Protection Act 2018 (the "**DPA**"). It relates to infringements of the General Data Protection Regulation (the "**GDPR**"), which came to the attention of the Information Commissioner ("**the Commissioner**").

1.2 The Commissioner considers that Ticketmaster was the controller, in respect of personal data of its customers, within the meaning of section 6 DPA and Article 4(7) GDPR, as Ticketmaster determined the purposes and means of the processing of the personal data. By, *inter alia*, performing operations or sets of operations on personal data such as collecting, storing and using the personal data of its individual customers, Ticketmaster is and was processing personal data within the meaning of section 3(4) DPA and Article (4)(2) GDPR.

1.3 This Penalty Notice arises out of an incident from 25 May 2018 to 23 June 2018, affecting personal data processed by Ticketmaster during that period (the "**Incident**"). The total duration of the personal data breach was between February 2018 and 23 June 2018 ("**the Personal Data Breach**"); however, the dates under consideration for the purposes of this Penalty Notice were from 25 May 2018 to 23 June 2018. Of the data subjects affected during the Incident:

1.3.1 9.4 million EEA data subjects were notified as having been potentially affected by the Personal Data Breach, of whom 1.5 million data subjects originated in the United Kingdom.

1.3.2 Barclays Bank have advised that around 60,000 individual card details had been compromised.

1.3.3 Monzo Bank have advised that around 6,000 cards have had to be replaced in relation to Ticketmaster transaction fraud.

1.3.4 Ticketmaster has received approximately 997 complaints alleging financial loss and/or emotional distress.

1.3.5 Ticketmaster have been unable to provide the Commissioner with a breakdown of the individuals affected during the period from 25 May 2018 to 23 June 2018.

1.4 For the reasons set out in this Penalty Notice, the Commissioner has found that Ticketmaster 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 appropriate technical and organisational measures as required by Article 5(1)(f) and Article 32 GDPR.

1.5 The Commissioner has found that, in all the circumstances, and having regard, in particular, to Ticketmaster's representations and the matters listed in Article 83(1) and (2) GDPR, the infringements constitute a serious failure to comply with the GDPR and, accordingly, that the imposition of a penalty is appropriate. The Commissioner has decided to impose a penalty under Article 83(5) GDPR. The amount of the penalty that the Commissioner has decided to impose is **£1,250,000.00**.

1.6 Pursuant to Article 54 GDPR, the Commissioner is acting as lead supervisory authority in respect of the cross-border processing at issue in this case with regard to Ticketmaster.

## 2 LEGAL FRAMEWORK

GDPR

2.1 On 25 May 2018, the GDPR entered into force, replacing the previous EU law data protection regime that applied under Directive 95/46/EC ("**Data Protection Directive**")[1]. The GDPR seeks to harmonise the protection of fundamental rights in respect of personal data across EU Member States and, unlike the Data Protection Directive, is directly applicable in every Member State.[2]

2.2 The GDPR was developed and enacted in the context of challenges to the protection of personal data posed by, in particular:

a. the substantial increase in cross-border flows of personal data resulting from the functioning of the internal market;[3] and

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[2] Recital 3.
[3] Recital 5.

b. the rapid technological developments which have occurred during a period of globalisation.[4] As Recital (6) explains: "*… The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities….*"

2.3 Such developments made it necessary for "*a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market…*".[5]

2.4 Against that background, the GDPR imposed more stringent duties on controllers and significantly increased the penalties that could be imposed for a breach of the obligations imposed on controllers (amongst others).[6]

The relevant obligations

2.5 Chapter 1 GDPR sets out the general provisions. Article 5 of Chapter II GDPR sets out the principles relating to the processing of personal data. Article 5(1) lists the six basic principles that controllers must comply with in processing personal data, including:

> *1. Personal data shall be:*
>
> *…(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*

2.6 Article 5(2) GDPR makes it clear that the "*controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*".

2.7 Chapter IV, Section 1 addresses the general obligations of controllers and processors. Article 24 sets out the responsibility of controllers for taking appropriate steps to ensure and be able to demonstrate that processing is compatible with the GDPR. Articles 28-29 make separate provision for the processing of data by processors, under the instructions of the controller.

---

[4] Recital 6.
[5] Recital 7.
[6] See, in particular, Recitals 11, 148, 150, and Article 5, Chapter IV and Article 83.

2.8 Chapter IV, Section 2 addresses security of personal data. Article 32 GDPR provides:

> *1. Taking into account the state of the art, the costs of of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) the pseudonymisation and encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) …*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.*
>
> *2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

2.9 Article 32 GDPR applies to both controllers and processors.

Penalties

2.10 Article 83(1) GDPR requires supervisory authorities to ensure that any penalty imposed in each individual case is "*effective, proportionate and dissuasive*".

2.11 The principle that penalties ought to be effective, proportionate and dissuasive is a longstanding principle of EU law. The Commissioner is under an EU law obligation to ensure that infringements of the GDPR are penalised in a manner that is effective, proportionate and dissuasive.

2.12 Further, Recital 148 emphasises, *inter alia*, that *"in order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation."* It also records that due regard should be given to the:

> *… nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor…*

2.13 Recital 150 provides as follows:

> *In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities*

*should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.*

2.14 In line with the above, when deciding whether to impose a fine and the appropriate amount of any such fine, Article 83(2) GDPR requires the Commissioner to have regard to the following matters:

*(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*

*(b) the intentional or negligent character of the infringement;*

*(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*

*(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*

*(e) any relevant previous infringements by the controller or processor;*

*(f) the degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*

*(g) the categories of personal data affected by the infringement;*

*(h) the manner in which the infringement became known to the supervisory authority, including whether, and if so to what extent, the controller or processor notified the supervisory authority of the infringement;*

*(i) where measures referred to in Article 58(2) have previously been ordered against the controller or*

*processor concerned with regard to the same subject-matter, compliance with those measures;*

*(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*

*(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, directly or indirectly from the infringement.* [7]

2.15 Article 83(5) GDPR provides that infringements of the basic principles for processing imposed pursuant to Article 5 GDPR will, in accordance with Article 83(2) GDPR, be subject to administrative fines of up to €20 million or, in the case of an undertaking, up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher.

2.16 Article 83(4) GDPR provides, *inter alia*, that infringements of the obligations imposed by Article 32 GDPR on the controller and processer will, in accordance with Article 83(2) GDPR, be subject to administrative fines of up to €10 million or, in the case of an undertaking, up to 2% of its total worldwide annual turnover of the preceding financial year, whichever is higher.

2.17 Article 83(3) GDPR addresses the circumstances in which the same or linked processing operations give rise to infringements of several provisions of the GDPR. It provides that "*… the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*".

2.18 Article 83(8) GDPR provides that the exercise by any supervisory authority of its powers to fine undertakings will be subject to procedural safeguards, including an effective judicial remedy and due process.

[7] See also the Article 29 Data Protection Working Party *Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679*, adopted on 3 October 2017, endorsed by the European Data Protection Board at its first plenary session. These provide a high-level overview of the assessment criteria set out in Article 83(2) GDPR in Section III ("**the Article 29 WP Guidelines**".

DPA

The Commissioner

2.19 Section 115 DPA establishes that the Commissioner is the UK's supervisory authority for the purposes of the GDPR. Section 115 DPA provides, *inter alia*, that the Commissioner's powers under Articles 58(2)(i) (the power to impose administrative fines) and 83 GDPR are exercisable only by giving a penalty notice under section 155 DPA.

Penalties

2.20 Section 155(1) DPA provides that, if the Commissioner is satisfied that a person has failed or is failing as described in section 149(2) DPA, the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice. This Penalty Notice has been issued pursuant to section 155(1) DPA.

2.21 Section 149(2) DPA provides:

> *(1) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following –*
>
> *(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);*
> *(b) …*
> *(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors)…*

2.22 Section 155 DPA sets out the matters to which the Commissioner must have regard when deciding whether to issue a penalty notice and when determining the amount of the penalty.

2.23 Section 155(2) DPA provides that, subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the matters listed in Article 83(1) and (2) GDPR.

2.24 Schedule 16 includes provisions relevant to the imposition of penalties. Paragraph 2 makes provision for the issuing of notices of intent to impose a penalty, as follows:

> *(1) Before giving a person a penalty notice, the Commissioner must, by written notice (a "notice of intent") inform the*

*person that the Commissioner intends to give a penalty notice.*

*(2) The Commissioner may not give a penalty notice to a person in reliance on a notice of intent after the end of the period of 6 months beginning when the notice of intent is given, subject to sub-paragraph (3).*

*(3) The period for giving a penalty notice to a person may be extended by agreement between the Commissioner and the person.*

2.25 Paragraph 5 sets out the required contents of a penalty notice, in accordance with which this Penalty Notice has been prepared.

Guidance

2.26 Section 160 DPA requires the Commissioner to produce and publish guidance about how she intends to exercise her functions. With respect to penalty notices, such guidance is required to include:

*(a) provision about the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice;*

*(b) provision about the circumstances in which the Commissioner would consider it appropriate to allow a person to make oral representations about the Commissioner's intention to give the person a penalty notice;*

*(c) provision explaining how the Commissioner will determine the amount of penalties;*

*(d) provision about how the Commissioner will determine how to proceed if a person does not comply with a penalty notice.*

2.27 Pursuant to section 161 DPA, the Commissioner's first guidance documents issued under section 160(1) DPA had to be consulted upon and laid before Parliament by the Secretary of State in accordance with the procedure set out in that section. Thereafter, in issuing any altered or replacement guidance, the Commissioner required to consult the Secretary of State and such other persons as she considers appropriate. The Commissioner must also arrange for such guidance to be laid before Parliament.

The Commissioner's Regulatory Action Policy

2.28 On 4 May 2018, the Commissioner opened a consultation process on how the Commissioner planned to discharge her regulatory powers under the DPA. The consultation attracted responses from across civil society, commentators, and industry (including the finance and insurance, online technology and telecoms, and charity sectors). The consultation ended on 28 June 2018. Having taken all the views received during the consultation process into account, the Regulatory Action Policy (the "**RAP**") was submitted to the Secretary of State and laid before Parliament for approval.

2.29 Pursuant to section 160(1) DPA, the Commissioner published her RAP on 7 November 2018. Under the hearing *"Aims"*, the RAP explains that it seeks to:

- *"Set out the nature of the Commissioner's various powers in one place and to be clear and consistent about when and how we use them";*
- *"Ensure that we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected";*
- *"Guide the Commissioner and our staff in ensuring that any regulatory action is targeted, proportionate and effective…"*[8]

2.30 The objectives of regulatory action are set out at page 6 of the RAP, including:

- *"To respond swiftly and effectively to breaches of legislation which fall within the ICO's remit, focussing on [inter alia] those adversely affecting large groups of individuals".*
- "*To be effective, proportionate, dissuasive and consistent in our application of sanctions",* targeting action taken pursuant to the Commissioner's most significant powers on, *inter alia, "organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data"*.

2.31 The RAP explains that the Commissioner will adopt a selective approach to regulatory action.[9] When deciding whether and how to

[8] RAP, page 5.
[9] RAP, pages 6-7 and 10.

respond to breaches of information rights obligations she will consider criteria which include the following:

- *"the nature and seriousness of the breach or potential breach";*
- *"where relevant, the categories of personal data affected (including whether any special categories of personal data are involved) and the level of any privacy intrusion";*
- *"the number of individuals affected, the extent of any exposure to physical, financial or psychological harm, and, where it is an issue, the degree of intrusion into their privacy";*
- *"whether the issue raises new or repeated issues, or concerns that technological security measures are not protecting the personal data";*
- *"the cost of measures to mitigate any risk, issue or harm";*
- *"the public interest in regulatory action being taken (for example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute)".*[10]

2.32 The RAP explains that, as a general principle, *"more serious, high-impact, intentional, wilful, neglectful or repeated breaches can expect stronger regulatory action".*[11]

2.33 Pages 24-25 of the RAP identify the circumstances in which the issuing of a Penalty Notice will be appropriate. They explain, *inter alia*, that in *"… considering the degree of harm or damage we may consider that, where there is a lower level of impact across a large number of individuals, the totality of that damage or harm may be substantial, and may require a sanction."* The RAP stresses that each case will be assessed objectively on its own merits. However, it explains that, in accordance with the Commissioner's risk-based approach, a penalty is more likely to be imposed in, *inter alia,* the following situations:

- *"a number of individuals have been affected";*
- *"there has been a degree of damage or harm (which may include distress and/or embarrassment);* and

[10] RAP, pages 10-11.
[11] RAP, page 12.

- *"there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it)".*

2.34 The process the Commissioner will follow in deciding the appropriate amount of penalty to be imposed is described from page 27 onwards. In particular, the RAP sets out the following five-step process:

a. **Step 1.** An 'initial element' removing any financial gain from the breach.

b. **Step 2.** Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) DPA.

c. **Step 3.** Adding in an element to reflect any aggravating factors. A list of aggravating factors which the Commissioner would take into account, where relevant, is provided at page 11 of the RAP. This list is intended to be indicative, not exhaustive.

d. **Step 4.** Adding in an amount for deterrent effect to others.

e. **Step 5.** Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship). A list of mitigating factors which the Commissioner would take into account, where relevant, is provided at page 11-12 of the RAP. This list is intended to be indicative, not exhaustive.

## 3 CIRCUMSTANCES OF THE FAILURE: FACTS

Background

3.1 This Penalty Notice does not purport to identify exhaustively each and every circumstance and document relevant to the Commissioner's proposal to give a penalty notice and considered by the Commissioner. The circumstances and documents identified below are a proportionate summary.

3.2 The Second Annex to this Penalty Notice provides a more detailed chronology.

Significant events prior to 23 June 2018

3.3 By Ticketmaster's written comments on the draft Penalty Notice ("**the Comments**"), it is stated that as early as 20 February 2018, Inbenta "*was aware of a potential compromise of its code*" (§18 of the Comments).

3.4 On 6 April 2018, around 50 customers of Monzo Bank ("**Monzo**") reported fraudulent transactions on their accounts, following which their payment cards were replaced.

3.5 On 12 April 2018, representatives of Ticketmaster met with Monzo at Monzo's offices to share information gathered by Monzo concerning the fraudulent transactions in issue.

3.6 On or around 16 April 2018, Monzo provided Ticketmaster with unique information regarding a particular payment card. When the legitimate customer tried to make the purchase on the Ticketmaster website, the customer accidentally inputted the expiry date of the relevant payment card incorrectly so the transaction failed. That same payment card and incorrect expiry date was then used in an attempted fraudulent transaction the following Monday. Monzo described this as *"smoking gun"* proof that Ticketmaster's website was the source of the Personal Data Breach.

3.7 On 17 April 2018, Barclaycard contacted Live Nation Entertainment (the ultimate parent company of Ticketmaster's corporate group) stating "*… we are aware of a breach occurrence within your Australian entity/unit ["**the Australia Event**"], is this something we should be aware of for the UK entity or is there any further information we need to know at this point?".*

3.8 Between 19 and 20 April 2018, Monzo made the decision to replace 6,000 payment cards used by customers on Ticketmaster's website.

3.9 By a published statement on Monzo's website, Monzo stated that on 19 April 2018 Ticketmaster informed Monzo that an internal investigation found no evidence of a personal data breach and that no other banks were reporting similar patterns of fraudulent transactions.

3.10 On 19 April 2018, the Commonwealth Bank of Australia informed Ticketmaster of suspected fraud on 198 accounts that shared Ticketmaster as a common purchase point.

3.11 During this same period Barclaycard, MasterCard and American Express reported to Ticketmaster suggestions of fraud.

3.12 On 27 April 2018, Monzo reported to Ticketmaster a sharp decline in fraudulent transactions since the replacement of payment cards of customers previously used on Ticketmaster's website.

3.13 On 1 May 2018, the Commonwealth Bank of Australia provided Ticketmaster with data concerning 1,756 MasterCard users who had been victims of fraud and who had all transacted on Ticketmaster's Australian website.

3.14 On or around 5 May 2018, Ticketmaster engaged four third party forensics firms (together "**the Incident Response Team**") to investigate the Australia Event and any data breach and subsequent fraud. The Incident Response Team analysed data provided by the Commonwealth Bank of Australia and determined that any breach of Ticketmaster's systems most likely originated out of Ticketmaster's Australian website, which was largely housed in North American networks and data centres.

3.15 On 6 May 2018, an individual user on Twitter tweeted a picture of an error message on the Ticketmaster New Zealand website. The tweet stated: *"… Inbenta's website serves two different files…hosted on two different servers one of them has the infected line in it and the other one doesn't."* This tweet should have been reasonably understood to refer to malicious code.

3.16 On 9 May 2018, the same Twitter user followed up that tweet. Ticketmaster responded directly to the tweet saying *"this is not a virus, it's the help widget that is found on our home page".*

3.17 On the same day, the Twitter user responded to Ticketmaster, stating: *"it has an extra line in it submitting information to a website hosted by an External person in the UAE and none of the other inbenta.js files used by other sites have this – this single one has been compromised."*

3.18 On or around 10 May 2018, Visa contacted Ticketmaster identifying a number of indicators of compromise and that fraud could be caused by malicious third party content.

3.18.1 Thereafter, Ticketmaster provided Visa's information to the Incident response Team.

3.18.2 However, Ticketmaster's instructions as to the scope of analysis to third party content by the Incident Response Team did not extend at that stage to payment systems within the United Kingdom and EU markets.

3.18.3 Further, Ticketmaster have not evidenced that a link was identified between the information received from Monzo (see above) and that from Visa regarding the Personal Data Breach arising from third party malicious scripts.

3.19. On 11 May 2018, the Incident Response Team analysed Visa's indicators of compromise and failed to identify the malicious code in issue.

3.20. On 31 May 2018, an individual using the Ticketmaster Ireland Website disclosed that their antivirus product had identified Ticketmaster's website as malicious, in particular the reference to the Inbenta tag.

3.21. On 1 June 2018, Ticketmaster internally reported that *"the worst-case scenario is that they* [Inbenta] *are indeed hacked/infected and serving up rogue malicious content to our userbase."*

3.22. On 6 June 2018, a Twitter user provided information to Ticketmaster that he was *"getting lots of Symantec alerts"* about the chat bot in Australia.

3.23. On 6 June 2018, following a telephone call the previous day, Inbenta emailed Ticketmaster to indicate that the identification of Ticketmaster's website as malicious by an antivirus product was erroneous.

3.24. On or around 6 June 2018, Ticketmaster nevertheless instructed the Incident Response Team to expand its investigations to include all Ticketmaster domains.

3.25. On or around 8 June 2018, the Incident Response Team reported that it had scanned 117 terabytes of data to search for malware and found no indication of malware.

3.26. On 22 June 2018 at 8.53pm, Ticketmaster received a notification from Barclaycard regarding around 37,000 instances of known fraud. As set out below, this is the date from which Ticketmaster has stated that it had knowledge of the Personal Data Breach in its personal data breach reports submitted to the Commissioner.

Discovery and reporting of the breach

3.27. By an email dated 23 June 2018 at 23.14pm, Ticketmaster attached a formal personal data breach notification.

3.27.1 The attached personal data breach report recorded that the breach was discovered on 22 June 2018 at 8.53pm.

3.27.2 The personal data breach report provided:

*"We were Notified by a third party card issuer that it has identified approximately 37,000 credit and debit cards that appear to have been compromised where Ticketmaster UK CPP [meaning "common point of purchase"] was involved. We are not aware of an actual breach or misuse of any credit or debit cards. We are in the process of investigating the matter and we are working with forensic investigators to identify any potential compromise of credit or debit card numbers."*

3.27.3 As to the issue of delay in reporting the Personal Data Breach, the personal data breach report provided: *"While we have been notified of a possible compromise, because there has been no confirmation of a breach, there has been no delay in reporting."*

3.27.4 Under the heading *"Taking action"*, the personal data breach report provided: *"We have engaged a and applications*

*leading forensics firm to conduct a full review of our systems to identify and remediate any potential vulnerabilities related to the potential exposure of the credit and debit cards identified by the third party card issuer."*

3.28 As around 1pm on 23 June 2018, malicious code on Ticketmaster's website was identified. That malicious code was fully disabled for all territories save for Ticketmaster France and getmein.com.

3.29. As to the malicious code:

3.29.1 Ticketmaster had contracted with Inbenta Technologies Inc ("Inbenta") to provide it with a chat bot for the Ticketmaster websites pursuant to contractual terms requiring software provided by Inbenta to be, amongst other things, free from malware. The chat bot on Ticketmaster's website was designed to interpret user's questions, to which it automatically identified relevant help articles or information. The automatic process was operated by a computer code that analysed questions.

3.29.2 The JavaScript for the chat bot was hosted on the Inbenta server. However, Ticketmaster decided to include the chat bot on various pages of its website, including the payment page. Ticketmaster said that the chat bot was a critical part of the customer's journey.

3.29.3 It was because of Ticketmaster's business decision to include the chat bot on its payment page that the chat bot was able to unlawfully process the personal data of customers. An attacker directed its attack at the Inbenta servers and inserted malicious code into the JavaScript for the chat bot. The malicious code 'scraped' (i.e. collected for the purpose of sending the data back to the attacker) user-inputted personal data. Because Ticketmaster included the chat bot on its payment page, the personal data scraped by the malicious code included financial data such as names, payment card numbers, expiry dated and CVV numbers.

3.30 On 4 June 2018, the chat bot was disabled for Ticketmaster France and getmain.com.

3.31 On 25 and 26 June 2018, Ticketmaster provided the Commissioner with verbal updates as to the steps then being taken by Ticketmaster to investigate the Personal Data Breach.

3.32 On 27 June 2018, Ticketmaster publicly disclosed the Personal Data Breach. On the same date, it sent the Commissioner a written update on how the incident was progressing.

3.33 In a statement responding to the Personal Data Breach on or around 27 June 2018, the CEO of Inbenta, told Register UK: *"... The Javascript we created specifically for Ticketmaster was used on a payments page, which is not what it was built for. Had we known that script would have been used in that way, we would have advised against it, as it poses a security threat."* For the reasons stated in the paragraph below, the Commissioner does not need to form a concluded view as to the veracity of Inbenta's statement.

3.34 It is recognised that Ticketmaster engaged with Inbenta, as outlined at §§34-43 of the First Representations. It is further recognised that Ticketmaster alleges that, in the context of Inbenta having been in breach of its contractual obligations to Ticketmaster to keep its software free from malware, certain responses of Inbenta were false or materially inaccurate and had been for an extended period. However, such responses of Inbenta were of minimal causal relevance including because the attack vector of the Personal Data Breach was not novel in type, and it had been notified to Ticketmaster otherwise than by Inbenta (including on Twitter, as to which see Ticketmaster's response to the tweet and clarification sought by Ticketmaster above). Insofar as the Comments (e.g. at §2.1 and §18) assert that Inbenta's failure to act on its alleged awareness of the unauthorised code within the chat bot "*directly caused the Incident*", that submission is rejected for the same reason.

3.35 By 28 June 2018, all potentially impacted data subjects were emailed to inform them of the Personal Data Breach.

3.36 On 29 June 2018, Ticketmaster sent the Commissioner an updated personal data breach notification.

3.36.1 The updated personal data breach report stated: *"We were notified by a third party card issuer that it has identified approximately 37,000 credit and debit cards that appear to have been compromised where Ticketmaster UK CPP was involved. Following on-going forensic investigations, we have discovered that a malicious script was introduced by a customer support product ("Chat Bot"), that was running on the Ticketmaster UK website.*

*The malicious script was Found on UK: https://ticketmasteruk.inbenta.com/avatar/jsonp/inbenta.js and appears to add an event listener to intercept all form posts. The Chat Bot product was hosted by a third party supplier, Inbenta Technologies, Inc. ("Inbenta"). The malicious code that was enabled in the product allowed an unauthorised third party to export customers' data. As soon as this breach was identified, the Chat Bot was removed from all [Ticketmaster International] sites."* [2]

3.36.2 The dates of the breach were stated to have been 10 February 2018 to 23 June 2018.

3.36.3 Ticketmaster stated that it had *"notified approximately 9.4 million international customers to let them know that they could possibly have been [affected]. All have been sent email notifications."*

3.36.4 Further information was provided concerning the action taken by Ticketmaster, which included:

*"- An email notification was sent to all customers 27-28 June 2018 who purchased or attempted to purchase tickets between February 10, 2018 and June 23, 2018. We have notified 9.4 million international customers.*

3.37 By a letter dated 29 June 2018, the Commissioner informed Ticketmaster that the case required further investigation. Further information was sought therein.

3.38 By a letter dated 13 July 2018, Ticketmaster responded to the Commissioner's letter dated 29 June 2018.

3.38.1 Ticketmaster explained the operation of the chat bot as follows:

*"… 3. Inbenta Technologies provided Ticketmaster with a number of services, including a chatbox service (the "Inbenta Chatbot"). The Inbenta Chatbot provided a customer service interface with Ticketmaster's customers on certain Ticketmaster platforms. The Inbenta Chatbot was active on some international Ticketmaster pages by default, so the user did not need to engage with the Inbenta Chatbot for it to be operational.*

*In summary, the Inbenta Malicious Code was present in the Inbenta Chatbot in certain, but not all instances, where the Inbenta Chatbot was operational. Based on the information available to Ticketmaster it appears that the Inbenta Malicious Code was capable of capturing any data input by user into Ticketmaster websites where the Inbenta Malicious Code was operational. Accordingly we assess that the Inbenta Malicious Code was capable of capturing customers' personal data, including name, address, email address, full credit card number, CVV, and Ticketmaster username and password, and sending them to the attacker. …"*

3.38.2 Ticketmaster stated that, as of 13 July 2018, approximately 500 complaints had been received by it.

3.38.3 Further, Ticketmaster stated: *"As part of Ticketmaster's GDPR readiness programme, Ticketmaster invested £2.5 million on an internal privacy portal to deal with data subject rights issues, including complaints."*

3.39 By a letter dated 1 October 2018, Ticketmaster provided an *"overview of developments in Ticketmaster's investigation into the data security incident that we reported to you on 23 June 2018."* A 28 page schedule accompanied Ticketmaster's letter dated 1 October 2018.

3.39.1 At paragraph 25 of that Schedule, Ticketmaster stated: *"… at no point did the Inbenta chatbot software itself load from or*

*reside within Ticketmaster's systems. Instead, it was at all times served directly to Ticketmaster's customers by Inbenta from Inbenta's servers. …"*

3.39.2 At paragraph 26 of that Schedule, Ticketmaster stated: *"… Ticketmaster considers the fact that it did not itself process any data as a result of the deployment of the chatbot and was otherwise constrained in its ability to manage the security controls placed around the software, must inevitably influence the question of the extent to which it can properly be held responsible for the data event."*

3.39.3 At paragraph 66 of that Schedule, Ticketmaster stated: *"In conclusion, Ticketmaster readily acknowledges that very unfortunately this attack exposed the personal and payment card data of a number of its customers (though not as many as Ticketmaster had originally understood could have been impacted). However, for all the reasons set out above, Ticketmaster believes that it would be unfair and unreasonable to lay the blame for this event at its feet. Put simply, this attack did not come about as a result of Ticketmaster applying a sub-standard, inappropriate approach to data security. To the contrary, this incident affected Ticketmaster's website* notwithstanding *its deployment of extensive appropriate measures designed to safeguard Ticketmaster customers from attack."* [Emphasis original]

3.40 By a letter dated 23 November 2018, Ticketmaster provided further information in response to the Commissioner's letter dated 9 November 2018. Ticketmaster stated:

[redacted]

3.41 By a letter dated 29 November 2018, the Commissioner requested further information from Ticketmaster. By a letter dated 7 December 2018, Ticketmaster provided further information in response to the Commissioner's letter dated 29 November 2018. The information so provided included information concerning the chat bot provided by Inbenta. Ticketmaster stated:

*"The chatbot provided by Inbenta Technologies ("Inbenta") and deployed on certain Ticketmaster webpages was a customer support tool that enabled customers to quickly and easily obtain "self-service" customer support. The chatbot was deployed on payment and checkout pages, consistent with industry practice, not to collect cardholder data, but to instead allow customer's access to quick customer service support at critical junctures within the payment purchase process. It was not intended to and did not in fact store, process or transmit cardholder data subject to the Payment Card Information Data Security Standard ("PCI-DSS"). Against this background, Ticketmaster did not query with Inbenta whether PCI-DSS would be applied in respect of the chatbot, instead, Ticketmaster sought to assure itself that the chatbot would not itself process or transmit payment card data. ….Relying on Inbenta's attestations as to the operation of the chatbot, and also the parties' mutual understanding of the chatbot's purpose and functionality, Ticketmaster reasonably did not require the Inbenta chatbot to maintain compliance with PCI-DSS. The tactics of the criminal actors who infected the Inbenta chatbot with malicious code so as to facilitate their own independent collection of cardholder data directly from customers were unusual and innovative, and could not have been reasonably anticipated."*

3.42 By a letter dated 18 December 2018, the Commissioner requested further information from Ticketmaster. By a letter dated 21 January 2019, Ticketmaster provided further information in response to the Commissioner's letter dated 18 December 2018. Ticketmaster stated: *"When companies like Ticketmaster contract with third parties to provide third-party software, the contracting company rarely has*

*visibility into the changes made to third-party scripts served from the TPV's [i.e. third party vendor] own servers."*

The Payment Card Industry Data Security Standard

3.43 The Payment Card Industry Data Security Standard ("**PCI-DSS**") was the security standard to which all merchants processing payment cards were required to adhere. PCI-DSS Version 3.2 was released in April 2016 and applied until 31 December 2018. PCI-DSS Version 3.2.1 was released May 2018 and is the current version of the standard.

3.44 The PCI DSS provided that "*the PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment.*" Systems components included: (i) systems that provided security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or might have impacted upon the security of the card data environment ("**CDE**"); (ii) applications including all purchased and custom applications, including internal and external applications; and (iii) any other component or device located within or connected to the CDE.

3.45 The chat bot in issue, when configured on a payment page, fell within the scope of the term "*system components*".

3.46 Ticketmaster has provided evidence, for example at §32.3 of its First Representations, that it intended that the chat bot was to be used on its payment page: the chat bot was to "*improve the online sales journey, through and including the checkout process—and the payment pages within it*".

3.47 In the course of the Information Commissioner's investigation, Ticketmaster provided its Secure Coding Guidelines, which provided at page 3: "*all internet-facing applications and applications with a PCI compliance requirement must also go through an application security assessment by the internal LNE Application Security Team OR by an approved external third party.*"

3.48 In those circumstances, despite its repeated contention to the contrary (including at §35 of the Comments) Ticketmaster was bound by the following PCI-DSS requirements concerning the payment card environment, which applied regardless of whether the chat bot was or was not intended or expected to process payment card information:

3.48.1 PCI DSS requirement 12.2 required Ticketmaster to *"implement a risk assessment process that: … is performed at least annually and upon significant changes to the environment. … identifies critical assets, threats and vulnerabilities."* However, no such risk assessment was performed upon the chat bot being introduced as part of the payment environment.

3.48.2 PCI-DSS requirement 12.8.2 required Ticketmaster to *"maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment."* However, notwithstanding Ticketmaster's submissions at Comments §13, the contract between Inbenta and Ticketmaster did not have such specific provisions concerning the security of payment card data.

3.48.3 PCI-DSS requirement 12.8.4 required Ticketmaster to *"maintain a program to monitor service providers' PCI DSS compliance status at least annually"*. However, Ticketmaster did not maintain such a programme.

3.48.4 PCI-DSS requirement 12.4 required Ticketmaster to *"Ensure that the security policy and procedures clearly define information security responsibilities for all personnel".* However, the contract between Inbenta and Ticketmaster lacked such clear definition of the information security responsibilities in relation to payment card data.

3.48.5 PCI DSS requirement 12.6 required Ticketmaster to *"implement a formal security awareness program to make all*

*personnel aware of the cardholder data security policy and procedure."* It is further provided: *"If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions."* However, Ticketmaster have failed to demonstrate a security awareness programme demonstrating which party was responsible for the security of the payment card data in relation to the chat bot.

3.49 In its letter of 7 December 2018, Ticketmaster confirmed that it *"is not aware of any accreditation held by Inbenta which attest to its compliance with PCI DSS".* The following further passages are noted:

3.49.1 *"Inbenta has consistently stated to Ticketmaster that their product did not store, process or transmit cardholder data and were thus not subjected to PCI-DSS"*

3.49.2 *"[The chatbox] was not intended to and did not in fact store, process or transmit cardholder data subject to the Payment Card Information Data Security Standard ("PCI-DSS")". Against this background, Ticketmaster did not query with Inbenta whether PCI-DSS would be applied in respect of the chatbox."*[12]

3.50 The Ticketmaster/Inbenta contract did not include any contractual provisions specifically in relation to the payment environment. Notwithstanding, in its Representations and the Comments, Ticketmaster asserts that it was entitled to rely on Inbenta to provide a safe chat bot on account of Inbenta being *"a reputable specialist software company that passed Ticketmaster's vetting procedures … [which had] provided assurances about the safety of its software and services. Those assurances were reflected in contractual commitments imposed on Inbenta"* (§7 of the Comments).

[12] It is recognised that Ticketmaster engaged with Inbenta, as outlined at §§34-43 of the First Representations. It is further recognised that Ticketmaster alleges that certain responses of Inbenta were false or materially inaccurate.

3.51 In its letter of 21 January 2019, Ticketmaster was unable to demonstrate that it had carried out a formal risk assessment of the implementation of the chat bot on its payment page, contrary to (amongst other things) Ticketmaster's own Secure Coding Guidelines.

3.52 By reason of the aforesaid, it was or ought to have been apparent to Ticketmaster that the security of the chat bot was not to a PCI-DSS compliant standard, including by reason of Ticketmaster's own failure to discharge its obligations under the PCI-DSS. Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the GDPR's security principle,[13] as Ticketmaster processed card data and suffered a personal data breach, the ICO considered the extent to which Ticketmaster might have put in place measures that PCI-DSS required, particularly given the breach related to a lack of a particular control or process mandated by the standard.

## 4 PERSONAL DATA INVOLVED IN THE FAILURE

4.1 As explained in Ticketmaster's letter of 13 July 2018, referred to above, customer's personal data that was the subject of the breach included *"name, address, email address, full credit card number, CVV, and Ticketmaster username and password".*

4.2 Whilst the total duration of the Personal Data Breach was between February 2018 and 23 June 2018, the dates under consideration for the purposes of this Penalty Notice were from 25 May 2018 to 23 June 2018.

4.2.1 9.4 million EEA data subjects were notified as having been potentially affected by the Personal Data Breach, of whom 1.5 million data subjects originated in the United Kingdom.

4.2.2 Barclays Bank have advised that around 60,000 individual card details had been compromised.

[13] At §33 of the Comments, Ticketmaster mischaracterises the Commissioner's conclusion when describing the Commissioner as having held *"that the GDPR required Ticketmaster to have applied PCI DSS to the Chatbot."*

4.2.3 Monzo Bank have advised that around 6,000 cards have had to be replaced in relation to Ticketmaster transaction fraud.

4.2.4 Ticketmaster has received approximately 997 complaints alleging financial loss and/or emotional distress.

4.3 Ticketmaster have been unable to provide the Commissioner with a breakdown of the individuals affected during the period from 25 May 2018 to 23 June 2018.

## 5 PROCEDURE

5.1 This section summarises the procedural steps the Commissioner has taken. The Second Annex to this Penalty Notice provides a more detailed chronology. All Ticketmaster's representations have been taken into account by the Commissioner when deciding to impose the penalty herein.

5.2 Ticketmaster initially notified the Commissioner of the Attack on 23 June 2018 by an email of 23:14 attaching a formal personal data breach notification. In response, the Commissioner commenced an investigation into the incident. That investigation included various exchanges with Ticketmaster and considering detailed submissions and evidence.

5.3 On 7 February 2020, the Commissioner issued Ticketmaster with a Notice of Intent to impose a penalty, pursuant to section 155(1) DPA and Schedule 16 of the DPA (the **"NOI"**). The proposed penalty at that stage was £1,500,000.

5.4 Ticketmaster made written representations in response to the NOI on 6 April 2020 and 22 May 2020, which are referred to in this Notice as "**Ticketmaster's First Representations**" and "**Ticketmaster's Second Representations**" respectively.

5.5 Ticketmaster's First Representations included:

5.5.1 At §3.3, Ticketmaster submitted: "*Viewed holistically, the security measures adopted by Ticketmaster were reasonable,*

*proportionate and appropriate, given the risk-landscape faced by Ticketmaster at the time*"

5.5.2 At §§3.1 and 3.2, Ticketmaster submitted that: (i) the chat bot was served by a third party, Inbenta; (ii) Ticketmaster had entered into a contract with Inbenta whereby Inbenta undertook that the chat bot would remain free from all malware, and (iii) Inbenta was at all material times well aware that the chat bot was to be used by Ticketmaster on its payment page.

5.5.3 At §3.5, Ticketmaster submitted that "*the risk that criminals would gain access to the personal data of Ticketmaster customers by attacking JavaScript software authored and served by a trusted third-party software provider from the third party's own servers was not something that could reasonably have been foreseen by Ticketmaster*". Ticketmaster contended that it was the "*victim of a novel form of criminal attack*". The contention that the attack vector was novel was repeated in the First Representations, e.g. at §§5.3 and 13-15.

5.5.4 At §4, Ticketmaster further summarised its criticisms of the Commissioner's conclusions on breach in the NOI as follows:

> *"4.1 They rest on the application of an unduly high security standard, well beyond that which is typically practised in the online service industry and that which is required under Articles 5(1)(f) and 32 GDPR;*
>
> *4.2 They depend on flawed assumptions as to the feasibility and effectiveness of various technical measures; and*
>
> *4.3 They are predicated on an analysis of the underlying facts which cannot be squared with the evidence."*

5.5.5 Further:

5.5.5.1 At §§18-23, Ticketmaster submitted that it had met its GDPR obligations by establishing "*adequate, proportionate measures to ensure that Inbenta's offerings were, and would remain, secure.*"

5.5.5.2 At §24, Ticketmaster submitted that the Commissioner's conclusions in the NOI required that "*Ticketmaster had to actively review each iteration of the Chatbot to comply with*

*Articles 5(1) and 32 GDPR*". Ticketmaster did not accurately represent the content of the NOI when so asserting.

5.5.5.3 From §28, Ticketmaster identified allegedly "*false and misleading*" statements of Inbenta in respect of the Incident.

5.5.5.4 From §54, Ticketmaster alleged errors by the Commissioner on the application of Article 33 GDPR. As to Ticketmaster's submissions in this regard, paragraph 6.29 of this Penalty Notice is repeated.

5.5.6 At §7, Ticketmaster submitted alternative "*inevitabl[e]*" conclusions, as a consequence of which it contended at §8 that the findings on breach in the NOI ought to be withdrawn:

> "*7.1 Along with those of its customers who were affected by the Inbenta Data Security Incident, Ticketmaster is the victim of a criminal attack perpetrated on a third-party software provider, which attack could not have been foreseen or prevented by Ticketmaster, applying appropriate security measures;*
>
> *7.2 Responsibility for the attack lies first and foremost on the shoulders of the Unknown Criminal Actors. Thereafter, it lies, if anywhere, on Inbenta's shoulders. There is no just basis for holding Ticketmaster liable; and*
>
> *7.3 Ticketmaster's approach to detecting the attack and its source cannot be impugned. It adopted a proportionate approach to identifying possible anomalies, relying (as it was entitled to do) on representations it received from Inbenta, all of which indicated the Chatbot remained secure. As soon as it was provided with reasonable evidence that an attack on its customers was underway, Ticketmaster commenced an appropriate and well-resourced investigation. It cannot be faulted merely because its conscientious and reasonable investigations arguably could have been prioritised differently, had an alternative initial focus or scope, or did not immediately identify the attack and its source."*

5.5.7 At §9 and §§74-80, Ticketmaster submitted that, without prejudice to its denial of breach of its GDPR obligations, in the NOI the Commissioner had adopted an erroneous approach to the application of the factors identified in Article 83(2) GDPR.

5.5.8 At §10, Ticketmaster submitted: "*without prejudice to the foregoing … even if there was a lawful basis for imposing a penalty, which there is not, the quantum of the proposed penalty should be reduced.*"

5.6 Ticketmaster also raised various requests for further particulars and documents in the First Representations. The Commissioner responded to the requests for further particulars and documents in the First Representations by email on 5 June 2020 ("**the RFI Response**"). Ticketmaster responded in turn on 17 June 2020 ("**Ticketmaster's Third Representations**").

5.7 The Commissioner's position on the substance of the matters in issue was informed, in particular, by careful consideration of Ticketmaster's First, Second and Third Representations (together "**the Representations**"). Given the length and detail of the Representations and the overall complexity of the case, that consideration took time and considerable resources. That process also resulted in changes and clarifications to the form and content of the draft decision.

5.8 On 29 April 2020, the Commissioner invited Ticketmaster to make further representations specifically in respect of the financial impact on its business caused by the Covid-19 pandemic Ticketmaster provided an initial written response to this request on 22 May 2020, and additional submissions by way of a telephone call on 26 May 2020 (together "**the Financial Impact Representations**").

5.9 On 19 August 2020 the Commissioner provided Ticketmaster with a draft Penalty Notice. The Commissioner invited Ticketmaster to make further representations as to the draft Penalty Notice.

5.10 On 16 September 2020, Ticketmaster provided the Comments, which were expressly without prejudice to the Representations.

5.11 By the Comments, Ticketmaster denied the Commissioner's findings of violations of Article 5(1)(f) and 32 GDPR. Ticketmaster alleged four "*fundamental flaws*", namely that: "*Inbenta's failures caused the Incident*"; "*the Incident was not reasonably foreseeable*"; "*Ticketmaster's security measures were appropriate*"; and "*the ICO's penalty analysis is flawed*".

5.12 As to causation, Ticketmaster alleged that the Commissioner "*neglects to address Inbenta's failures and their causation of the Incident adequately, or at all*". Ticketmaster asserts that it was

*"entitled to rely on Inbenta, as a reputable specialist software company, to provide the Chatbot, particularly in light of the assurances Inbenta had provided, and the contractual guarantees Ticketmaster had in place with Inbenta."*

5.13 As to reasonable foreseeability, Ticketmaster alleges that Commissioner has engaged in "*hindsight bias*".

5.14 As to Ticketmaster's security measures, Ticketmaster objects to *"(i) the ICO's conclusion that the GDPR required Ticketmaster to have applied PCI DSS to the Inbenta Chatbot; (ii) the DPN's failure to take into account or properly weigh Inbenta's contractual assurances to Ticketmaster that the Chatbot would be free of malicious code and Inbenta's breach of those obligations; (iii) the DPN's silence on industry practice regarding the deployment of JavaScript on payment pages; and (iv) the ICO's position on the reasonableness/appropriateness of the mitigation measures suggested in the DPN."*

5.15 As to the Commissioner's penalty analysis, Ticketmaster identifies various alleged flaws, including: *"(i) Live Nation Entertainment's "financial picture" is irrelevant to the ICO's penalty analysis; (ii) the DPN's finding of "negligence" is overly broad and ripe to be misinterpreted as a finding of common law negligence, which finding the ICO has no jurisdiction to make; (iii) the DPN fails to reflect the fact that there has been no evidence in the course of the ICO's investigation that the data subjects affected by the Incident suffered any harm and (iv) the DPN fails to apply a discount in respect of the amount of the penalty originally suggested to reflect the fact that the ICO has abandoned the allegation that Ticketmaster breached Article 33 GDPR."*

## 6 CIRCUMSTANCES OF THE FAILURE: BREACHES

Ticketmaster's failures

6.1. The Commissioner's conclusion is that in respect of the Incident, Ticketmaster had failed to comply with its obligations under Article 5(1)(f) and Article 32 GDPR. Ticketmaster 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

appropriate technical and organisational measures as required by Article 5(1)(f) and Article 32 GDPR.

6.2. This section describes the specific failures to comply with the GDPR that the Commissioner has found and responds to Ticketmaster's Representations concerning the Commissioner's NOI.

The relevant standard

6.3. As set out above, Article 5 GDPR requires that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The data controller, in this case Ticketmaster, is responsible for, and must be able to demonstrate compliance with, that requirement.

6.4. Article 32 GDPR concerns the security of processing personal data and, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, requires a controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Such measures may include encryption of personal data and a process for regularly testing, assessing and evaluating the effectiveness of such technical and organisational measures.[14]

6.5. Not every instance of unauthorised processing or breach of security will necessarily amount to a breach of Article 5 or Article 32. The obligation under Article 5 GDPR is to ensure *appropriate* security; the obligation under Article 32 is to implement *appropriate* technical and organisational measures to ensure an *appropriate* level of security, taking account of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk to the rights of data subjects.

6.6. When considering whether there has been a breach of the GDPR and whether to impose a penalty, the Commissioner must therefore avoid reasoning purely with the benefit of hindsight. The Commissioner has been mindful of that at all times when considering the Incident. The focus has been on the adequacy and

[14] See also Recitals 76, 77 and 83 GDPR.

appropriateness of the measures implemented by the data controller, the risks that were known or could reasonably have been identified or foreseen, and appropriate measures falling within Article 5 and/or Article 32 GDPR that were not, but could and should have been, in place. The Commissioner has identified those measures that were proportionate in the circumstances, taking into account that it was open to Ticketmaster at all times not to include the chat bot on its payment page at all.

6.7. Having carefully examined the available evidence, including the evidence and submissions set out in Ticketmaster's Representations, the Commissioner is satisfied that there were multiple failures by Ticketmaster to put in place appropriate technical or organisational measures to protect the personal data being processed on Ticketmaster's systems, as required by the GDPR.

6.8. The NOI identified a number of failures by Ticketmaster to put in place appropriate security measures (certain of which were identified by way of illustration), including Ticketmaster's failure to put in place appropriate measures to negate the risk from the danger of third party scripts infecting the chat bot on the payment page of Ticketmaster's website. Following careful consideration of the detailed representations received from Ticketmaster, the principal failures Ticketmaster (which are now the subject of this Penalty Notice) are outlined below.

Revised scope of the findings made

6.9. In the NOI, concerns were raised in relation to Article 33 GDPR. In the NOI, the Commissioner identified that Ticketmaster had failed to notify the Commissioner of the Personal Data Breach without undue delay and in any event within 72 hours of becoming aware of the breach, as required by Article 33 GDPR. For the purposes of this Penalty Notice, the Commissioner does not rely on any breach of Article 33 GDPR and any prior finding of a breach of Article 33 GDPR no longer forms part of the decision against Ticketmaster.

6.10. Subject to the paragraph immediately above and the RFI Response, the Commissioner repeats and relies upon the NOI.

Ticketmaster's principal failures

6.11. Ticketmaster has failed to comply with the requirements of Article 5(1)(f) GDPR, including to process personal data *in a manner that ensures appropriate security of the data, including protection*

*against unauthorised or unlawful processing, using appropriate technical or organisational measures."* Whilst some measures were in place prior to the Personal Data Breach, they were insufficient in the circumstances.

6.12. Ticketmaster has failed to comply with the requirements of Article 32(1) and (2) GDPR. In particular:

6.12.1 Article 32(1)(b) GDPR required Ticketmaster to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. By reason of such obligations, in particular concerning integrity, Ticketmaster was required to ensure that only authorised changes were made to Ticketmaster's website that processed personal data, including the payment pages.

6.12.2 Article 32(1)(d) GDPR required that Ticketmaster had a process for regular testing, assessing and evaluating the effectiveness of technical and organisational controls for ensuring the security of processing.

6.13 By Article 32 GDPR, *"the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk",* taking into account *"the state of the art".*

6.14 The state of the art includes knowledge, actual and constructive, of attack vectors (i.e. pathways to a target or the methods used by an attacker to compromise a target) current at the date of the Personal Data Breach and whether the measures in response to those attacks are adequate in line with the state of current technologies.

6.15 Implementing third party JavaScripts into a website or chat bot has, for some time, been a known security risk. The risk to personal data is greater when such third party JavaScripts are implemented into web pages that process personal data such as a payment page. Extensive publications had addressed that risk and identified associated security measures in advance of the Personal Data Breach in this instance. In particular, publications had identified that a benign script could be changed by an attacker to 'scrape' personal data, of which process the data controller or processor would likely have no visibility.

6.16 Publications evidencing that the risk of implementing third party

JavaScripts into a web site or chat bot were identified in the RFI Response. These publications, in conjunction with the PCI-DSS standard, demonstrate that the risk from third party scripts was well-established within the cyber and payment card security industry. The actor vector leading to the data breach was not novel in type and, prior to the breach, there were publications clearly indicating the risk of including third party scripts on a payment page,[15] as illustrated by publications including:

6.16.1 "*Risks with third party scripts on Internet Banking Sites*" of September 2014, at https://marc.durdin.net/2014/09/risks-with-third-party-scripts-on-internet-banking-sites/:

> *"So what's the big deal with running third party script on a website?*
>
> *The core issue is that scripts from third party sites can be changed at any time, without the knowledge of the ANZ Internet Banking team. In fact, different scripts can be served for different clients — a smart hacker would serve the original script for IP addresses owned by ANZ Bank, and serve a malicious script only to specific targeted clients. There would be no reliable way for the ANZ Internet Banking security team to detect this."*

6.16.2 "*NIST 800-161*" of April 2015 at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf, including at page 1, Chapter 1:

> *"ICT Supply Chain risks include insertion of counterfeits, unauthorised production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practises in the ICT supply chain. These risks are realised when threats in the ICT Supply chain exploit existing vulnerability."*

6.16.3 "*Does including all these 3rd party Java script files impose a security risk*", of November 2015, at

[15] C.f. §14.3(i) of the First Representations: "*The specific attack vector pursued by the Unknown Criminal Actors was novel and was not widely known or discussed in the industry.*"

https://stackoverflow.com/questions/33878372/does-including-all-these-3rd-party-javascript-files-impose-a-security-risk:

*"When you have all these various javascript files included on a page for various services like website analytics, click tracking etc., doesn't this create a huge security risk because using javascript they can hijack the person's credit card that is entered on the form?*

*How is this even considered to be safe currently?*

*Yes this is a security risk, known as a third party script include.*

*By including a script on your page hosted by a 3rd party, you are trusting that the external domain is not malicious nor compromised. By using a <script src="//example.com"> tag, the third party domain has full control of the DOM on your site. They can inject whatever JavaScript they wish.*

*You are right to be concerned. PageFair was recently compromised bringing down every site that it offered its analytics service to with it. You should verify all third party domains that you are referencing for script, and ensure you trust them. For example you are probably OK with the big guys such as Google and Facebook, however any others you should consider either dropping them or reviewing the script code and then hosting locally on your domain instead."*

6.16.4 ENISA 2015 Threat Landscapes of January 2016 at https://www.enisa.europa.eu/publications/etl2015:

*"As a targeted attack, the threat agent performs different actions in order to obtain knowledge about the internal composition of the target organization: Personnel, organizational information, possible weaknesses, etc. to prepare an attack in a successful manner. Recognized attack vectors include infected media, supply chain compromise, and social engineering including combination of different attacks. The purpose of these attacks is to place custom malicious code on one or multiple computers for specific tasks and to remain undetected for the longest possible period."*

6.16.5 *"Things to know (and potential dangers) with third-party scripts"*, of June 2016, at https://css-tricks.com/potential-dangers-of-third-party-javascript/:

*"Any time you include someone else's external script on your page, there's an inherent security risk because that script has full access to the front end of your site."*

6.16.6 ENISA 2016 Threat Landscape of January 2017 at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017:

*"Targeted attacks are malicious attacks that are aimed to a specific individual, company, system or software based on some specific knowledge regarding the target…… Attack vector on targeted attacks uses to:*

- *Other sophisticated attacks can use infected media for circumvolving external network defences or for penetrating in to airgaps, and supply chains attacks"*

6.16.7 *"The Danger of Third Party Scripts"*, of February 2017, at https://blog.detectify.com/2017/02/02/the-danger-of-third-party-scripts/:

*"An external resource could change if the provider hosting the script gets hacked, or if they decide to go malicious and change it themselves. This introduces a single-point-of-failure situation, where an attacker could instead of hacking only you take the time and hack the hosting provider of the script and by doing so take control of all sites that include it."*

6.16.8 *"Protecting Your Customer's Payment Card Data from Malware"* of April 2017, at https://blog.pcisecuritystandards.org/infographic-protecting-your-payment-data-from-malware.

*"Hackers often target low hanging fruit;*

- *Weak or default passwords*
- *Outdated anti-virus software*
- *Unencrypted data*
- *Access via 3rd party vendors with weak security controls"*

(underlined by ICO for empathises)

*Here's what you can do right now…*

- *Confirm that all third party vendors are properly implementing and maintain security controls outlined in the PCI Data Security Standard (PCI DSS)"*

6.16.9 "*How companies are hacked via malicious Javascript"* of April 2017 at https://www.normshield.com/how-companies-are-hacked-via-malicious-javascript-code/:

*"One of the most sneaky uses of JavaScript is cross-site scripting (XSS). Simply put, XSS is a vulnerability that allows hackers to embed malicious JavaScript code into a legitimate website, which is ultimately executed in the browser of a user who visits the website. If this happens on a website that handles sensitive user information, such as financial data, the malicious code could potentially snoop and steal that information"*

6.16.10 ENISA 2017 Threat Landscape of January 2018 at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018:

*"Once again, in 2017 malware is the most frequently encountered cyberthreat. It continued its constant evolution in terms of sophistication and diversity….*

*The identified interesting points for malware are as follows:*

***Supply chain attacks:*** *one compromised vector can affect many organisations. Similar with enterprises which are looking to save time and money all the time, attackers are searching new ways to make their attacks more and more efficient. As the Cisco partner RSA discovered, supply chain attacks can offer maximize the impact with a minimal effort invested by the criminals. In the case that RSA handled, the attackers inserted*

*malicious codes into legitimate software typically used by system administrators to analyse Windows system logs. The compromised software was available for download at the vendor's website. The result was maximized because one compromised vector—the vendor site—could then spread the threat to many more enterprise networks, simply by allowing users to download the compromised software."*

6.16.11 NCSC Supply Chain of January 2018 at https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples.

"*A series of high profile, very damaging attacks on companies has demonstrated that attackers have both the intent and ability to exploit vulnerabilities in supply chain security. This trend is real and growing. So, the need to act is clear."*

Examples of Supply Chain attacks within the guidance;

*"Learn about an example of a supply chain attack through a third party software provider, where a legitimate industrial control system is 'trojanised " and "Cyber criminals also target supply chains as a means of reaching the broadest possible audience with their malware"*

6.16.12 ICO & NCSC GDPR Security Outcomes of May 2018[1] at https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes.

"*You have appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to personal data*

*A.4 Data processors and the supply chain*

*You understand and manage security risks to your processing operations that may arise as a result of dependencies on third parties"*

[1] This document was published during the period of the ongoing data breach in issue. In the course of its representations, Ticketmaster has relied upon the "*VISA Fraudsters Targeting Call Centres*" publication of July 2018. That publication post-dated the Incident. It is nevertheless noted that its relevant content is consistent with the publications identified in this Penalty Notice, which date from before or during the Incident.

6.17 Contrary to criticism of the NOI at §14 of the First Representations, those publications evidence that Ticketmaster ought reasonably to have been aware prior to the time of the Incident of the risk of implementing third party JavaScripts into a web site that processes personal data such as payment card data. Ticketmaster's challenges to the Commissioner's reliance on those publications in the Third Representations on the basis of their provenance, their date or their lack of specificity do not undermine the clear effect of those publications for the purposes of this Penalty Notice, namely the risk of implementing third party scripts was well established within the cyber and payment card security industry, with many websites, forums posts and news articles explaining the risks prior to the Incident. In that context, Ticketmaster's contention at §§27 and 29.4 of the Comments that the publication of the "*VISA Fraudsters Targeting Call Centres*" publication of July 2018 after the Incident "*was … to rectify an existing lack of knowledge among e-commerce merchants that third party JavaScript posed a serious risk to the security of payment pages*" such that the Incident could not be regarded as having been reasonably foreseeable at the relevant time is not accepted. Ticketmaster overstates the significance at §29.4 of the Comments of both the "*VISA Fraudsters Targeting Call Centres*" publication of July 2018 and the ICO's third party software guidance of July 2019 as marking a "*pivotal point*" (which, given the dates of publication of those documents, presumably is said to have lasted a year in duration) in the foreseeability of an attack like the Incident. Indeed, the relevant content of the "*VISA Fraudsters Targeting Call Centres*" publication of July 2018 is consistent with the publications identified at paragraph 6.16 above, which date from before or during the Incident.

6.18 The publications referred to at paragraph 6.16 above also demonstrate the range of technical measures that were available to Ticketmaster to mitigate or remove the risk of a third party script being implemented on a website or chat bot. At all times, it was open to Ticketmaster not to support the chat bot on the payment page of its website, which would have removed the risk of the attack vector being deployed.

6.19 Further, as set out above, it was well known in advance of the Personal Data Breach that, in efforts to attack organisations, attackers frequently target less secure third party organisations

supplying services to a primary organisation. Such attacks are referred to as supply chain attacks.

6.20 A data subject's personal payment card information includes some of the most valuable items of personal data to be targeted by an attacker. Whilst there are certain protections for consumers in the event of the exploitation of their payment card information in order to mitigate their risk of financial harm, the attacker potentially stands to obtain significant financial gains by obtaining payment card information: the incentive for the attacker is not meaningfully reduced by the protections for consumers. As such, the likelihood that an attacker will seek to direct an attack to scrape personal data on a payment page of a website is increased.

6.21 In view of the aforesaid, Ticketmaster ought to have been aware that the severity and likelihood of an attack to obtain personal data entered on the payment page of Ticketmaster's website were both high. Ticketmaster failed to comply with its requirements of Article 5(1)(f) GDPR to process personal data in a manner that ensures appropriate security, including because it had not put in place appropriate measures to negate the risk from the danger of third party scripts infecting the chat bot on the payment page of Ticketmaster's website. Ticketmaster should have addressed the following three objectives:

6.21.1 The security of the third party product, namely the Inbenta chat bot.

6.21.2 The implementation of the Inbenta chat bot into Ticketmaster's own infrastructure.

6.21.3 The on-going verification that security was being achieved to an acceptable level.

6.22 As to securing the Inbenta chat bot:

6.22.1 Ticketmaster failed to discharge its obligations under the PCI-DSS (as to which see further above).

6.22.2 Ticketmaster's Third Party Vendor ("**TPV**") Program had required Inbenta to undergo periodic security vetting in 2013

and in 2018. The intervals between the periodic security vetting were very extended in the circumstances of evolving threats. The 2018 vetting was only completed during the period of the Personal Data Breach. As such, at the commencement of the Personal Data Breach, the most recent completed periodic security vetting pursuant to the TPV Program had been completed in 2013.

6.22.3 At §§8-9 of its Comments, Ticketmaster relies upon its receipt of security certifications provided by Inbenta. At §29.3 of the Comments, Ticketmaster emphasises Inbenta's ISO 27001 certification. The Commissioner places little weight on the mere provision of such certifications by Inbenta as a mechanism of securing the chat bot in the circumstances. Further, ISO 27001 is an information security management standard, which does not apply directly to software development.

6.22.4 Ticketmaster has failed to evidence a business requirement document, or other formal document (such as that in paragraph 3.48.2 above), by which Inbenta was clearly and unambiguously obliged to design the chat bot for use on the payment page of Ticketmaster's website. The absence of a business requirement document is illustrative of Ticketmaster's failure to secure the chat bot appropriately in all the circumstances. Contrary to §15 of the Comments, the Commissioner does not find that the absence of a business requirement document is, of itself, such as to amount to a breach of the GDPR in every case.

6.22.5 Despite the notifications by, amongst others, Monzo and Commonwealth Bank of Australia of possible fraud involving the Ticketmaster website, the integrity of the chat bot was not initially checked, assessed or otherwise tested to ensure that it has not been compromised. Indeed, it took Ticketmaster approximately nine weeks from the date of Monzo's notification of possible fraud involving the Ticketmaster website for Ticketmaster to run a payment through its payment page and monitor the network traffic thereon.

6.22.6 Whilst the Commissioner acknowledges Inbenta's contractual obligations to Ticketmaster to keep its software free from malware and Ticketmaster's observations at Comments §13, Ticketmaster nevertheless failed to implement a layered approach to security, including by meeting the requirements of the PCI-DSS in relation to the chat bot. The Commissioner considered that, in light of the clear risk of third party scripts within a payment page, and the scale of personal data, including payment card data, processed on the payment page, such a layered approach to security, and compliance with the PCI-DSS in relation to the chat bot, was an appropriate level of security required.

6.22.7 In addition, Ticketmaster was notified of potential unauthorised access to its system from as early as 6 April 2018 by Monzo Bank. During the time period of 6 April 2018 to 10 May 2018 it received further notifications from Monzo Bank, Commonwealth Bank of Australia, Barclays, Mastercard and American Express, as to which see further above. Visa provided specific information to Ticketmaster that fraud could be occurring via malicious third party JavaScript content. A twitter user notified Ticketmaster explaining the malicious code was within the chat bot on the Ticketmaster website, and explained what it was doing. At no times during this time period did Ticketmaster take steps properly to verify the chat bot.

6.22.8 It was not until a member of the public explained the malicious code to Ticketmaster that Ticketmaster raised the issue with Inbenta. At no time did Ticketmaster verify the code was malicious itself.

6.22.9 That certain responses of Inbenta were then false or materially inaccurate and continued to be, including upon Ticketmaster having been notified of the attack vector of the Personal Data Breach otherwise than by Inbenta (including on Twitter, as to which see Ticketmaster's response to the tweet and clarification sought by Ticketmaster above) Ticketmaster continued to place undue reliance on Inbenta's contractual security obligations and failed to take sufficient

and timely steps of its own to address the security of the chat bot.

6.23. As to the implementation of the Inbenta chat bot into Ticketmaster's own infrastructure, the following illustrative proportionate steps that might have been taken by Ticketmaster have been identified:

6.23.1 Because a chat bot is not strictly necessary for the service of taking a payment, common industry guidance and standards did not recommend its inclusion on the payment page of a website. Ticketmaster, however, decided to include the chat bot on the payment page of its website. All third party scripts, save for a Google Analytics script, were removed from the payment page of Ticketmaster's website only after the Personal Data Breach. Removing the chat bot from the payment page from the outset is not a disproportionately burdensome measure.

6.23.2 Because the payment page processed personal data, Ticketmaster should have risk-assessed the implementation of third party scripts into this page. Ticketmaster have been unable to show threat analysis documentation or that they took into consideration the risk of implementing third party scripts into a webpage that processed personal data prior to the Personal Data Breach.

6.23.3 Ticketmaster have submitted emails which show it is likely that Inbenta were aware that the chat bot was to form part of the Ticketmaster customer experience, up to and including the payment page. Notwithstanding this, it was still the responsibility of Ticketmaster to put measures in place on its own payment page to address the documented risk of third party scripts. Technical measures in line with the state of the art were available to it, such as SRI. These measures could have significantly reduced the likelihood of a successful compromise of the personal data that Ticketmaster processed, even in light of Inbenta's security failings. Indeed this is the very issue that SRI seeks to address. That Inbenta knew of the chat bot on the payment page does not materially change this matter.

6.23.4 Ticketmaster was unable to demonstrate it had any other appropriate measures that would have provided a comparable level of protection taking into consideration the requirements of Article 32 of the GDPR.

6.24. As to on-going verification that security was being achieved to an acceptable level:

6.24.1. Ticketmaster provided no evidence to show that key performance indicators relating to the verification of the on-going security of the chat bot were used prior to the Personal Data Breach. Ticketmaster has not evidenced that it carried out reviews in such a way that would have detected and mitigated the risk of malicious code changes.

6.24.2. Ticketmaster confirmed that it had no visibility of changes to the script of the chat bot made by Inbenta prior to the Personal Data Breach. Any changes to the script would have been automatically applied without authorisation from Ticketmaster. Ticketmaster was therefore unable to understand fully or assess the risks posed to its systems or to ensure the ongoing integrity of it systems.

6.24.3. Ticketmaster did not adequately test, assess or evaluate whether the security measures operating between the chat bot and its own payment page were adequate to address the known risks of third party scripts. By way of illustration, the following were not undertaken:

6.24.3.1. Paragraphs 3.49 and 3.50 above are repeated. Ticketmaster did not perform an adequate risk assessment of the security measures operating between the chat bot and its own payment page prior to the implementation of the chat bot.

6.24.3.2. Further, no adequate security testing was carried out specific to the interaction between the third party application and the payment page after implementation of the chat bot, including a security assessment that assessed the security measures in

place that were designed to prevent or detect malicious changes to the chat bot.

6.24.3.3. Ticketmaster confirmed that sub-resource integrity (SRI)) had not been implemented prior to the Personal Data Breach.

6.24.3.4. In its letter dated 21 January 2019 Ticketmaster stated that SRI is not a workable solution for dynamic JavaScript because its domains are highly dynamic and that implementing SRI would pose enormous organisational challenges because Ticketmaster would be required to update SRI every time Inbenta changed the code.

6.24.3.5. Ticketmaster provided further information that it was unaware exactly how often Inbenta made any changes. Therefore it was unknown to Ticketmaster at the time whether this would impose enormous organisational challenges.

6.24.3.6. Furthermore, Ticketmaster was unable to demonstrate any formal decision making with regard to SRI. The Commissioner does not consider the mere fact that JavaScript may be used as a dynamic scripting language is, of itself, a proper reason not to implement SRI. The Commissioner and maintains that SRI was an appropriate measure with regard to the state of the art, taking into account the scale and sensitivity of the personal data within the Ticketmaster payment page.

6.24.3.7. In addition, Ticketmaster provided information that at the time of the Personal Data Breach more than half of its customers would have benefitted from the inclusion of SRI.

6.24.3.8. The ICO views this type of measure as an appropriate measure to implement in this circumstance.

6.24.3.9. In addition, other measures were also available to Ticketmaster that could have been used with, or independently from, SRI, namely local hosting, content security policies and iFrames, should Ticketmaster wish to have proceeded with the chatbox on the payment page without SRI.

6.24.3.10. Ticketmaster confirmed that it did not use local hosting of the script for the chat bot prior to the Personal Data Breach.

6.24.3.11. The Commissioner accepts that the script was not hosted locally and that Ticketmaster might have been entitled to allow Inbenta to host it, as is common with many other third party scripts.

6.24.3.12. However the Commissioner would expect that Ticketmaster would have implemented commonly used measures, such as SRI. Where Ticketmaster could not, the Commissioner would expect Ticketmaster to have been able to demonstrate why that was the case and clearly to show that it had taken into consideration other alternative and appropriate measures, such as CSP, iFrame, the local hosting of the script, which is now Inbenta's recommendation.

6.24.3.13. Ticketmaster confirmed that a content security policy was not used prior to the Personal Data Breach.

6.24.3.14. Ticketmaster did not use iFrames (i.e. a method of embedding a web page within another webpage such that one is isolated from another). In respect of iFrames, Ticketmaster provided information that it did not have in place iFrames at the time of the incident. It stated it used other security measures, such as a contract that the chat bot should remain free of malicious software, as an alternative. The Commissioner does not accept that this contract offered an alternative appropriate level of security comparable with solutions such as SRI and, iFrames.

6.24.3.15. In respect of a content security policy, Ticketmaster provided information that it implemented this after the Personal Data Breach, notwithstanding the removal of the chat bot.

6.24.3.16. The ICO would not expect Ticketmaster to undertake the type of white box testing described in its Representations, namely of the actual proprietary chat bot source code. However, it is relevant that Ticketmaster did not have a method in place to test the security measures between the chat bot and Ticketmaster's own payment page, and *a fortiori* was unable to identify whether such measures would have been adequate to mitigate the known risks.

6.25. Ticketmaster was unable to demonstrate it had any other appropriate measures that would have provided a comparable level of protection taking into consideration the requirements of Article 32 of the GDPR.

6.26. 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. Ticketmaster has shown very limited knowledge at the date of the Incident of the risk of implementing third party scripts into a payment page, despite it being widely known and documented at that time. *A fortiori*, Ticketmaster has not evidenced that it deployed appropriate and proportionate controls to manage this risk.

Article 33

6.27. At the NOI stage, a provisional finding of breach of Article 33 GDPR was proposed. However, this finding no longer forms part of the decision against Ticketmaster.

6.28. In reaching this decision, the Commissioner considered Ticketmaster's Representations[16] asserting that, for the purposes of identifying a breach of Article 33 GDPR: (i) the Commissioner had applied *"an incorrect standard for becoming "aware" of a breach"*; (ii) the Commissioner had not considered *"the significance of the Barclaycard notification that only occurred on 22 June 2018, or its resulting shift in investigative focus"*; and (iii) the Commissioner had *"rested on incorrect facts and unrealistic assumptions that unfairly second-guess the decisions that Ticketmaster made at the time as to how to direct its investigations."*

6.29. In this particular case, and in the context of Ticketmaster's Representations, the Commissioner has decided not to make a finding that Ticketmaster breached Article 33 GDPR.

## 7 REASONS FOR IMPOSING A PENALTY & CALCULATION OF THE APPROPRIATE AMOUNT

7.1 For the reasons set out above, the Commissioner's view is that Ticketmaster has failed to comply with Articles 5(1)(f) and 32 GDPR. These failures fall within the scope of section 149(2) and 155(1)(a) DPA. For the reasons explained below, the Commissioner has decided that it is appropriate to impose a penalty in the light of the infringements she has identified.

7.2 In deciding to impose a penalty, and calculating the appropriate amount, the Commissioner has had regard to the matters listed in Articles 83(1) and (2) GDPR and has applied the five-step approach set out in her RAP.

<u>The imposition of a penalty is appropriate in this case</u>

7.3 Both the RAP and Article 83 GDPR provide guidance as to the circumstances in which it is appropriate to impose an administrative fine or penalty for breaches of the obligations imposed by the GDPR.

7.4 Article 83(2) GDPR lists a number of factors that must be taken into account. These are each discussed in detail below in determining the appropriate level of fine, in accordance with the steps outlined in the RAP. The points made below are also relied upon in justifying the

[16] At §55ff of Ticketmaster's First Representations.

Commissioner's decision to impose a penalty, in the light of the findings of infringement set out above.

7.5 The RAP provides guidance on when the Commissioner will deem a penalty to be appropriate. In particular, the RAP explains that a penalty is more likely to be imposed where, *inter alia*, (a) a number of individuals have been affected; (b) there has been a degree of damage or harm (which may include distress and/or embarrassment); and (c) there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it).

7.6 Taking together the findings made above about the nature of the infringements, their likely impact, and the fact that Ticketmaster for the purposes of Article 83(2)(b) negligently (but not intentionally) failed to comply with its GDPR obligations, the Commissioner considers it appropriate to apply an effective, dissuasive and proportionate penalty, reflecting the seriousness of the breaches which have occurred.

Calculation of the appropriate penalty

Step 1: an 'initial element' removing any financial gain from the breach

7.7 Ticketmaster's 2018 Annual Report and Financial Statements are the most recent audited financial information available and have been relied upon by the Commissioner for the purposes of this Penalty Notice.[17] In those accounts, Ticketmaster's turnover was recorded as £102,912,000.00 with a post-tax loss of £22,548,000.00. £3,989,000.00 of legal costs were attributable to the Incident. No gain arising from the Incident can be identified.

[17] Ticketmaster's audited accounts for the period ending 31 December 2019 have not been filed at Companies House, nor have unaudited accounts been provided by Ticketmaster to the Commissioner for the purposes of the investigation of the Personal Data Breach and the setting of the penalty under Article 83(5) GDPR.

Step 2: Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at sections 155(2)-(4) DPA

7.8 Sections 155(2)-(4) DPA refer to and reproduce the matters listed in Articles 83(1) and 83(2).

***The nature, gravity and duration of the failure (Article 83(2)(a))***

7.9 This was a significant contravention of the GDPR. The Personal Data Breach continued from 25 May 2018 to 23 June 2018, during which period it remained undetected by Ticketmaster's systems.

7.10 During this time the attacker was potentially able to access the payment card details of approximately 9.4 million customers, of whom approximately 1.5 million were UK customers. Ticketmaster are unable to provide a breakdown of the number of affected customers pre- and post-GDPR.

7.11 As of 31 May 2018, reports had also been received by Ticketmaster from the Bank of Australia, MasterCard, Barclays, American Express and Monzo Bank, as well as Twitter users, all of whom informed Ticketmaster that it was the source of a payment card breach.

7.12 The Incident Response Team's instructions were ineffective in scope and depth and not all relevant information was provided initially.

7.12.1 The Incident Response Team's instructions were initially confined to Microsoft Windows systems. Third party content such as JavaScripts would not have been included within the scope of the Incident Response Team's instructions accordingly.

7.12.2 Had Ticketmaster requested the Incident Response Team to investigate the whole payment environment on Ticketmaster's website, that would have included any scripts within the payment page of the website and accordingly increased the likelihood that the mechanism of the Personal Data Breach would have been identified earlier.

7.12.3 The Incident Response Team suggested that the information initially received from Ticketmaster concerned the Australia Event alone.

7.12.4 Ticketmaster provided information from Visa to the Incident Response Team on 10 May 2018. Had Ticketmaster instructed the Incident Response Team to extend its investigations from the Australia Event to the EU/United Kingdom market, the prospects of identifying the Personal Data Breach earlier would have increased.

7.12.5 It was not until 6 June 2018 that Ticketmaster requested the Incident Response Team to investigate Ticketmaster's United Kingdom website.

7.12.6 The scope and depth of the investigations conducted by the Incident Response Team were limited accordingly.

7.13 Ticketmaster carried out passive monitoring of its payment page on 23 June 2018 by running card details through the payment page and monitoring network traffic. Had passive monitoring been undertaken in the first instance, there would have been an increased likelihood that the mechanism of the Personal Data Breach would have been identified earlier.

7.14 Ticketmaster failed to act in accordance with the PCI-DSS standard, as to which see further above.

***The intentional or negligent character of the infringement (Article 83(2)(b))***

7.15 The Personal Data Breach was not intentional or deliberate. However, Ticketmaster displayed a lack of consideration to protect personal data and was negligent for the purposes of Article 83(2)(b). It was negligent of Ticketmaster to presume, without adequate oversight or technical measures, that Inbenta could provide an appropriate level of security in respect of the processing of payment cards. In particular, Ticketmaster's breach of the PCI-DSS standard was negligent for the purposes of Article 83(2)(b).

7.16 The malicious actor took advantage of Ticketmaster's inability to detect changes to scripts on its payment page. Following industry

guidance could have mitigated this risk. Ticketmaster should have been aware of the risks to personal data in the circumstances.

7.17 The decision to install the chat bot on the payment page of Ticketmaster's website was an identified failure and gave rise to a risk of a personal data breach. That risk had been identified contemporaneously in publications, about the substance of which Ticketmaster ought to have had knowledge.

7.18 Controls were available to Ticketmaster that could have identified the breach, but they were not used for an extended period.

***Any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83(2)(c))***

7.19 Once Ticketmaster removed the chat bot from its website, the Breach ended.

7.20 Ticketmaster created a website where customers and media could receive information about the Personal Data Breach.

7.21 Ticketmaster arranged for 12 months of credit monitoring for individual affected.

7.22 Ticketmaster forced password resets across all of its domains.

7.23 [redacted]

7.24 It is noted that Ticketmaster has submitted at §75.2 of the First Representations that the small number of cards reported as compromised relative to the volume of transactions during the Incident should be regarded as a mitigating factor. That submission carries little weight. The raw number of affected or potentially affected individuals is very much more significant when assessing the gravity of the breach. In any event, the low ratio of affected cards as against the transaction volume is likely a feature of the intermittent attack vector, and not a consequence of any steps taken by Ticketmaster during the period of the Incident.

***The degree of responsibility of the controller or processor (Article 83)(2)(d))***

7.25 Ticketmaster failed in its obligations under Article 5(1)(f) and Article 21(1) GDPR and relevant sections of the DPA to have regard to considerations including the state of the art, likelihood of attack, its severity and what appropriate controls were available at the time.

7.26 In that regard, it is noted that Ticketmaster was entirely responsible for the security of its systems and the protection of personal data.

***Relevant previous infringements (Article 83(2)(e))***

7.27 No other compliance matters or infringements have been taken into account when setting the amount of the penalty.

***Degree of cooperation with supervisory authority (Article 83(2)(f))***

7.28 Ticketmaster has fully co-operated with the Commissioner during this investigation and has provided evidence upon request, save as to the financial information referred to below.

***Categories of personal data affected (Article 83(2)(g))***

7.29 As set out above, Ticketmaster have provided information that the personal data of approximately 9.4 million customers potentially affected was likely to have included basic personal identifiers (e.g. names and contact details), identification data (e.g. usernames and passwords), and financial data (e.g. bank details and credit card, debit card and CVV numbers).

***Manner in which the infringement became known to the Commissioner (Article 83(2)(h))***

7.30 Ticketmaster reported this incident to the Commissioner on 23 June 2018. However, as set out above, Monzo and other third parties informed Ticketmaster of a potential personal data breach as early as February 2018.

Conclusion at step 2

7.31 Taking into account: (a) the matters set out in the preceding sections of this Penalty Notice; (b) the matters referred to in this section; and (c) the need to apply an effective, proportionate and dissuasive fine in the context of a controller of Ticketmaster's scale and turnover, the Commissioner had considered that a penalty of £1,500,000.00 would have been appropriate. A penalty of that scale was referred to in the NOI. This amount was considered appropriate to reflect the seriousness of the breach and took into account in particular the need for the penalty to be effective, proportionate and dissuasive. As set out below, the penalty has since been revised downwards to £1,250,000.

Step 3: Adding in an element to reflect any aggravating factors (Article 83(2)(k))

7.32 The amount of the penalty, as identified at Step 2, may be increased where there are 'other' aggravating factors.[18] In this case, the Commissioner does not consider there to be any other relevant aggravating factors. Thus, no adjustment is made to the penalty level determined at Step 2.

Step 4: Adding in an amount for a deterrent effect on others

7.33 As to the need for an effective deterrent, the Commissioner considers that a fine, accompanied by appropriate communications in accordance with the Communicating Regulating Enforcement Action Policy, would serve as an effective deterrent.

[18] In accordance with Article 83(2)(k) GDPR, section 155(3)(k) DPA, and page 11 of the RAP.

Step 5: Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship) (Article 83(2)(k))

7.34 The Commissioner has considered the following mitigating factors:

7.34.1 The facts and matters set out below under the sub-heading "Ticketmaster's other representations on the decision to impose a penalty and the appropriate Penalty amount", which are relevant to the issue of financial hardship.

7.34.2 Once Ticketmaster removed the chat bot from its website, the Personal Data Breach ended.

7.34.3 Ticketmaster forced password resets across all of its domains.

7.34.4 The Commissioner is not aware of any outstanding compliance matters that would suggest that further steps to mitigate the damage or distress suffered by data subjects are required.

7.34.5 Ticketmaster created a website where customers and media could receive information about the Personal Data Breach.

7.34.6 Ticketmaster has incurred considerable costs in relation to the Infringement, including the cost of twelve months of credit monitoring offered to all affected customers and legal costs.

7.34.7 [redacted]

7.35 By its Comments, Ticketmaster notes that "*there has been no evidence in the course of the ICO's investigation that the data subject affected by the Incident suffered any harm*". The

Commissioner does not regard the absence of harm upon a data breach to be, of itself, a mitigating factor in the circumstances of the Personal Data Breach.

Application of the fining tier(s) (Articles 83(4) and (5) GDPR)

7.36 The infringement of Article 5(1)(f) GDPR falls within Article 83(5)(a) GDPR, whereas Article 32 falls within Article 83(4)(a). The appropriate tier is therefore that imposed by Article 83(5)(a) as this is the gravest breach in issue in this case.

Ticketmaster's other representations on the decision to impose a penalty and the appropriate Penalty amount

7.37 Ticketmaster's Financial Impact Representations included:

7.37.1 Ticketmaster's primary business is the marketing and sale of tickets to live spots, music and entertainment events.

7.37.2 [redacted]

7.37.3 Ticketmaster observed that nearly all events in the second, third and fourth quarters of 2020 have been cancelled or rescheduled to 2021 by reason of Covid-19. [redacted]

7.37.4 [redacted]

7.37.5 [redacted]

7.37.6 In light of Covid-19, Ticketmaster had taken steps to reduce its operating costs, including by way of salary cuts, cancellation of events, and extensive staff furloughing.

7.37.7 [redacted] Ticketmaster submitted that: "*… given the unprecedented decline in Ticketmaster's anticipated Q2-Q4 ticket sales precipitated by COVID-19, it would be disproportionate and unjust for the ICO calculate a proposed penalty based on 2018 or 2019 revenues under Article 83(4).*"

7.37.8 Ticketmaster relied upon the Commissioner's statement dated 15 April 2020 entitled "*The ICO's regulatory approach during the coronavirus public health emergency*", including the acknowledgment therein that: "*the current coronavirus public health emergency means that … organisations are facing acute financial pressures impacting their finances and cashflows.*" The statement further provided: "*… before issuing fines we take into account the economic impact and affordability. In current circumstances, this is likely to mean the level of fines reduces.*"

7.37.9 Ticketmaster requested that the Commissioner eliminate or reduce the proposed £1,500,000 penalty "*to account for the significant financial challenges faced by Ticketmaster as a result of the COVID-19 pandemic. … Under these exceptional circumstances, Ticketmaster respectfully submits that the £1.5 million penalty proposed in the NOI is no longer proportionate under Article 83(1) GDPR, based on Ticketmaster's anticipated 2020 revenues.*"

7.38 The Commissioner has had regard to the impact of Covid-19 on Ticketmaster and the continuing uncertainty resulting therefrom, as described in Ticketmaster's Financial Impact Representations, including:

7.38.1 It is clear that the penalty of £1,500,000.00 proposed in the NOI would add to Ticketmaster's predicted operating loss.

7.38.2 Ticketmaster asserts that the Covid-19 pandemic has had a substantial impact on its business. [redacted]

[redacted]

7.38.3 [redacted] Ticketmaster presents no figures or evidence to support these statements.

7.38.4 Ticketmaster provided some limited additional information, explaining that [redacted], compared to an operating profit of around £4,000,000 in 2018. No detail or explanation has been provided to support these assertions.

7.38.5 Despite the detailed questions sent to Ticketmaster by the Commissioner, it has not provided any details on its debt position or liquidity.

7.39 Notwithstanding, the Commissioner has had regard to Ticketmaster's failure to answer some questions in relation to costs and failure to provide more general information as to its financial position and the government support it is presently receiving.

7.40 Having regard to the exceptional circumstances prevailing as a consequence of the Covid-19 pandemic, the Commissioner has decided to make a proportionate reduction in the penalty from £1,500,000 to £1,250,000. The Commissioner notes with respect to the revised penalty sum:

7.40.1 Having considered Ticketmaster's Financial Impact Representations, the Commissioner finds that

Ticketmaster has the financial means to be able to pay the penalty.

7.40.2 The Commissioner's policy "*The ICO's regulatory approach during the coronavirus public health emergency*" (published on 13 July 2020 at https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf) provided:

"*We will be flexible in our approach, taking into account the impact of the potential economic or resource burdens our actions could place on organisations.*

*… the ICO will continue to act proportionately, balancing the benefit to the public of taking regulatory action against the potential detrimental effect of doing so, taking into account the particular challenges being faced at this time. …*

*7. As set out in the Regulatory Action Policy, before issuing fines we take into account the economic impact and affordability. In current circumstances, this is likely to mean the level of fines reduces."*

7.40.3 Taking into account the Commissioner's regulatory approach during the Covid-19 pandemic, an exceptional reduction of the proposed penalty by £250,000 was determined to be proportionate. The penalty sum is accordingly **£1,250,000**.

## 8 HOW THE PENALTY IS TO BE PAID

8.1 The penalty must be paid to the Commissioner's office by BACS transfer or cheque by 15 December 2020 at the latest. The penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

## 9 ENFORCEMENT POWERS

9.1 The Commissioner will not take action to enforce a penalty unless:

- the period specified within the notice within which a penalty must be paid has expired and all or any of the penalty has not been paid;
- all relevant appeals against the penalty notice and any variation of it have either been decided or withdrawn; and
- the period for appealing against the penalty and any variation of it has expired.

9.2 In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Dated the 13th day of November 2020

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

**ANNEX 1**

## RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 162(1) of the Data Protection Act 2018 gives any person upon whom a penalty notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that she ought to have exercised her discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   General Regulatory Chamber

   HM Courts & Tribunals Service

   PO Box 9300

   Leicester

   LE1 8DJ

   a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;

h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).

**Annex 2**

**Chronology**

Part 1: Chronology of information in relation to the incident prior to Ticketmaster reporting personal data breach to ICO.

Part 2: Chronology of information in relation to the ICO's investigation into the personal data breach ("the Breach").

# Part 1:

10 February 2018: An unknown attacker injected malicious code into an Inbenta hosted chat bot. At the time of the attack, the chat bot was added on to Ticketmaster payment page. The malicious code extracted copies of any data submitted on the payment page including payment card data.

20 February 2018: By Ticketmaster's Comments at §18, it is stated that as early as 20 February 2018, Inbenta "*was aware of a potential compromise of its code*".

06 April 2018: 50 customers contacted Monzo Bank ("Monzo") to report fraudulent transactions on their account. On investigation, Monzo's Financial Crime and Security Team reported that 70% of the customers affected had shopped at Ticketmaster previously. Monzo reported that this was unusual as overall only 0.8% of all their customers had used this merchant.

7-8 April 2018: Monzo recorded a further four fraudulent transactions, of which two had previously used Ticketmaster.

12 April 2018: Monzo reported to Ticketmaster that they were trying to contact them regarding suspected fraudulent activity but were unable to get further than the Ticketmaster customer service team.

Ticketmaster responded on the same day and arranged a same day meeting.

12-16 April 2018: Monzo reported eight other attempted fraudulent transactions of which six had previously been used by Ticketmaster.

16 April 2018: Monzo provide Ticketmaster with information regarding one particular payment card that was unique. On 07 March 2018 a legitimate customer tried to make the purchase on the Ticketmaster website and accidentally inputted the expiry date so the transaction failed. The attacker would have been unaware the transaction had failed – they would have just received the card number with the incorrect expiry date. That same payment card and incorrect expiry data was then used in an attempted fraudulent transaction on 12 March 2018.

16 April 2018: Monzo provide information to Ticketmaster on how they were able to detect the trend: to summarise, Monzo were able to carry out real time monitoring.

At the same time Monzo supplied information to Ticketmaster that, during April 2018, 70% of all its fraudulent transactions occurred from customers who had previously shopped at Ticketmaster. It provided further information that these Ticketmaster transactions occurred within clusters of dates. Monzo explained this was evidence that Ticketmaster was the source of the breach.

19 April 2018: Monzo reported to Ticketmaster a further 11 compromised cards, all of which had previously used Ticketmaster.

19 April 2018: Monzo reported an additional 20 compromised cards, all of which had previously had purchases from Ticketmaster.

19 April 2018: Monzo reported to Ticketmaster that they had made the decision to replace 6,000 payment cards of customers that have previously shopped at Ticketmaster.

19 April 2018: Ticketmaster were notified of suspected fraud by the Commonwealth Bank of Australia ("CBA") containing 198 accounts that shared Ticketmaster as the common purchase point ("the Australia breach").

During the period between 19 April 2018 and 26 April 2018 Barclays, MasterCard and American Express suggested to Ticketmaster that fraudulent activity involving Ticketmaster was occurring.

27 April 2018: Monzo reported to Ticketmaster that they had noticed a sharp decline in fraudulent transactions since mass replacement of the payments card of customers that had previously shopped at Ticketmaster.

01 May 2018: CBA provided information to Ticketmaster that 1,756 Mastercard users had been victims of fraud, all of whom had undertaken recent transactions on Ticketmaster's Australian website.

03 May 2018: Ticketmaster engaged four third party forensic firms ("the incident response team") to investigate the Australia breach.

06 May 2018: A security researcher contacted Ticketmaster New Zealand via Twitter stating that he believed there was malicious code contained within the chat bot.

09 May 2018: Ticketmaster had not responded to this tweet. The Twitter user prompted Ticketmaster for a response. On the same day Ticketmaster replied providing information that it was not malicious code but was the chat bot.

09 May 2018: Twitter user replied advising Ticketmaster that they were incorrect and malicious code was in the chat bot. They provided information that there was a line of code that was submitting information to a website hosted by an external person in the UAE. The Twitter user also informed Ticketmaster that the scripts were hosted on two different servers, one of which was infected (i.e. some customers would receive the correct chat bot, and some would receive the malicious chat bot).

Ticketmaster confirmed that they would investigate the matter.

10 May 2018: Visa provided Ticketmaster information that the fraud could be caused by malicious third-party content.

10 May 2018: Ticketmaster raised the issue of malicious code with Inbenta.

15 May 2018: Inbenta confirmed the issue was fixed and provided information that the malicious code was due to a *"bad deployment of the code".*

15 May 2018: Ticketmaster replied to Inbenta's email asking why there was a line of code that was sending data to the UAE. In this email, Ticketmaster stated that *"we are not techs so the [previous] information doesn't mean a great deal."*

22 May 2018: Ticketmaster reported to Inbenta that the malicious code was back.

30 May 2018: Inbenta reported to Ticketmaster that *"the Ticketmaster avatar was built along time ago and is not using the latest application version and this is the reason why some suspicious code is injected there".*

31 May 2018: Another individual who had been using the Ticketmaster Ireland website disclosed that his antivirus product was flagging up the website as malicious, in particular regarding the chat bot and malicious network traffic.

31 May 2018: In reply to the information Ticketmaster received on 31 May 2018 internal emails show that Ticketmaster's Information Security team was aware of anti-virus products detecting the Inbenta Chat bot as malicious on multiple occasions. It stated that *"we've had this a few times now from Inbenta"* and that *"the worse case scenario is that they*

[Inbenta] *are indeed hacked/infected and serving up rogue malicious content to our userbase"*

01 June 2018: Ticketmaster confirmed via email that Inbenta had fixed the link in the past but "*somehow it gets changed*". In the same email, Ticketmaster confirmed that only Norton AV picks up the link as malicious. Ticketmaster stated that the

06 June 2018: Another Twitter user provided information to Ticketmaster that he was "*getting lots of Symantec alerts*" about the chat bot in Australia. (Symantec is an Anti-Virus provider)

06 June 2018: Following a telephone call the previous day, Inbenta emailed Ticketmaster to indicate that the identification of Ticketmaster's website as malicious by an antivirus product was erroneous.

06 June 2018: Ticketmaster instructed the incident response team to expand the investigation from Australia to all Ticketmaster domains. The incident response team undertook this within the scope of their contract with Ticketmaster.

08 June 2018: Ticketmaster reported that the incident report team had scanned 117 terabytes of data to search for malware and found no indication of malware. Ticketmaster reported that it was advised to "discontinue the hunt".

22 June 2018: Barclays contacted Ticketmaster to make it aware of 37,300 instances of known fraud from customers that had used Ticketmaster between February-June 2018.

23 June 2018: Ticketmaster ran a payment through the UK Ticketmaster payment page and monitored the data flow. Ticketmaster detected that the data was being sent to a foreign domain, which it later confirmed as belonging to the attacker.

23 June 2018: The chat bot was fully disabled for all the territories save for France which was disabled on the 24 June 2018.

# Part 2:

23 June 2018: Ticketmaster submitted a personal data breach ("PDB") notification to the ICO.

26 June 2018: Barclays provided the ICO with information on how the Breach came to light and the effect on Barclays' customers. It advised that other banks had also seen similar fraudulent activity on their cards, which appeared to be linked to Ticketmaster.

27 June 2018: Ticketmaster reported to the the ICO that it was in the process of notifying customers in the UK regarding the Breach as per its Article 34 requirements.

27 June 2018: Ticketmaster provided the ICO with a copy of its data subject notification.

27 June 2018: Ticketmaster provided the ICO with an update as to the status of its internal investigation into the Breach.

29 June 2018: Ticketmaster provided the ICO with an updated PDB report.

29 June 2018: ICO issued the first letter of enquires to TM (technical and data protection questions).

13 July 2018: Ticketmaster responded to the ICO letter of 29 June 2018.

13 July 2018: Ticketmaster provided the ICO with a timeline of the Breach as per its internal investigation.

27 July 2018: Ticketmaster provided a further response to the ICO's letter of 29 June 2018.

27 July 2018: Ticketmaster provided information from Inbenta in relation to the Breach.

01 August 2018: ICO issued the second letter of enquiry to TM establishing data subject locations.

06 August 2018: Ticketmaster responded to the ICO letter 01 August 2018.

08 August 2018: ICO issued the third letter of enquires to TM (technical and data protection questions).

10 August 2018: Ticketmaster responded to the ICO letter 29 June 2018.

22 August 2018: Ticketmaster responded to the ICO letter 08 August 2018.

01 October 2018: Ticketmaster provided the ICO with an update relating to key facts of its internal investigation into the Breach.

09 November 2018: ICO issued the fourth letter of enquires to TM (technical and data protection questions).

13 November 2018: Ticketmaster responded to the ICO letter 09 November 2018.

23 November 2018: Ticketmaster provided further responses to the ICO letter 09 November 2018.

29 November 2018: ICO issued the fifth letter of enquires to Ticketmaster (technical and data protection questions).

18 December 2018: ICO issued the sixth letter of enquires to Ticketmaster (technical and data protection questions).

21 January 2019: Ticketmaster responded to the ICO letter 18 December 2018.

28 February 2019: ICO issued the seventh letter of enquires to Ticketmaster.

21 March 2019: ICO issued the eighth letter of enquires to Ticketmaster.

07 February 2020: ICO issued Notice of Intent to Ticketmaster with a proposed penalty of £1,500,000.

13 February 2020: Ticketmaster requested an extension to respond to the Notice of Intent.

24 February 2020: ICO Director of Investigations authorised the extension.

07 April 2020: Ticketmaster submitted representations in relation to the Notice of Intent issued to it on 07 February 2020. In its representations, Ticketmaster also requested further information from the ICO in relation to aspects of the Notice of Intent.

22 May 2020: Ticketmaster submitted financial representations in relation to the impact of COVID-19.

5 June 2020: ICO issued further information to Ticketmaster in relation to its requests for further information.

08 June 2020: Ticketmaster requested an extension in relation to responding to the further information submitted to it on 5 June 2020.

08 June 2020: ICO Director of Investigations authorised a one week extension.

17 June 2020: Ticketmaster submitted further representations in relation to the Notice of Intent.