AN A.S. PRATT PUBLICATION
JANUARY 2021
VOL. 7 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: PRIVACY IN THE NEW YEAR
Victoria Prussen Spears

COULD FILLING OUT A FANTASY FOOTBALL LINEUP LAND YOU IN FEDERAL PRISON?
Josh H. Roberts

CAN CALIFORNIA'S PRIVACY INITIATIVE REVITALIZE U.S.-EU COMMERCE? Dominique Shelton Leipzig, David T. Biderman, Chris Hoofnagle, and Tommy Tobin

CALIFORNIA AG SETTLEMENT SUGGESTS PRIVACY AND SECURITY PRACTICES OF DIGITAL HEALTH APPS MAY PROVIDE FERTILE GROUND FOR ENFORCEMENT ACTIVITY
Elizabeth H. Canter, Anna D. Kraus, and Rebecca Yergin

BRITISH AIRWAYS FACES SIGNIFICANTLY REDUCED FINE FOR GDPR BREACH
Huw Beverley-Smith, Charlotte H.N. Perowne, and Fred Kelleher

DESIGNING A BIPA DEFENSE: USING ARBITRATION AGREEMENTS AND CLASS ACTION WAIVERS TO LIMIT BIPA LIABILITY
Jeffrey N. Rosenthal and David J. Oberly

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 1** **JANUARY 2021**

Editor's Note: Privacy in the New Year
Victoria Prussen Spears 1

Could Filling Out a Fantasy Football Lineup Land You in Federal Prison?
Josh H. Roberts 3

Can California's Privacy Initiative Revitalize U.S.-EU Commerce?
Dominique Shelton Leipzig, David T. Biderman, Chris Hoofnagle, and Tommy Tobin 15

California AG Settlement Suggests Privacy and Security Practices of Digital Health Apps May Provide Fertile Ground for Enforcement Activity
Elizabeth H. Canter, Anna D. Kraus, and Rebecca Yergin 20

British Airways Faces Significantly Reduced Fine for GDPR Breach
Huw Beverley-Smith, Charlotte H.N. Perowne, and Fred Kelleher 24

Designing a BIPA Defense: Using Arbitration Agreements and Class Action Waivers to Limit BIPA Liability
Jeffrey N. Rosenthal and David J. Oberly 28

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [245] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

British Airways Faces Significantly Reduced Fine for GDPR Breach

By Huw Beverley-Smith, Charlotte H.N. Perowne, and Fred Kelleher*

Despite a huge reduction from the initial fine amount, the £20 million fine imposed on British Airways remains the largest fine ever issued by the U.K.'s Information Commissioner's Office for a breach of the General Data Protection Regulation and is a clear statement of the seriousness it places on data processing responsibilities. The authors of this article discuss the fine and the wider implications.

At £20 million, the fine imposed on British Airways ("BA") for its infringement of the General Data Protection Regulation ("GDPR") is the biggest fine of its kind in the history of the U.K.'s Information Commissioner's Office ("ICO"). While markedly lower than the fine initially proposed, the process by which the revised figure was reached provides some interesting insights on the factors that regulators will take into account and is a clear sign that despite the current economic climate, the ICO is not afraid to enforce strict GDPR compliance.

On October 16, 2020, the U.K.'s data protection regulator, the ICO, gave notice of the fine to be imposed on British Airways for a customer data breach that occurred between June and September 2018 ("Penalty Notice"). The ICO found that BA had failed significantly in its role as a data controller to preempt and prepare its security measures against a highly sophisticated cyberattack.

Yet the reduction in the fine issued from the initially proposed £183.39 million is confirmation of the significant financial benefit that can be gained from full cooperation with an investigation, and an indication of the ICO's ongoing adaptability in its enforcement of the General Data Protection Regulation 2016/679 during a time of continued disruption by COVID-19.

---

* Huw Beverley-Smith is a partner in Faegre Drinker's London office, where he advises customers and suppliers on a range of international transactions and regulatory issues, including technology, telecommunications and business process outsourcing, complex services agreements, intellectual property ownership and licensing, and privacy and cybersecurity. Charlotte H.N. Perowne is an associate in Faegre Drinker's London office, where she advises clients on a range of international transactions and regulatory issues, including technology transactions, outsourcing, intellectual property ownership and licensing, data privacy, and cybersecurity. Fred Kelleher is a trainee solicitor in Faegre Drinker's London office, where he advises clients on emerging legal and regulatory trends relating to labor and employment. The authors may be reached at huw.beverley-smith@faegredrinker.com, charlotte.perowne@faegredrinker.com, and fred.kelleher@faegredrinker.com, respectively.

Across Europe, data protection authorities ("DPAs") such as the ICO have made statements to confirm that they will ensure to continue to act in the public interest throughout the COVID-19 pandemic. During this time, that means they should retain the right balance, focusing on those areas likely to cause the greatest public harm and recognizing the genuine constraints on most businesses, which will inevitably impact their ability to fully comply with all aspects of the law. Generally, there is an expectation of more action from DPAs right across Europe, the COVID-19 pandemic notwithstanding, as companies that have thus far been given the benefit of the doubt and assistance with compliance are increasingly subjected to tougher enforcement action.

BACKGROUND TO THE ICO'S PENALTY NOTICE

The initial Notice of Intent to fine BA £183.39 million (equating to 1.5 percent of BA's worldwide turnover in 2017) was issued following the airline's failure to prevent a cyber incident that compromised over 500,000 customers' personal details in 2018. This would have been the largest fine (by a significant margin) imposed by any EU data protection regulator.

The attack involved a sophisticated infiltration of BA's systems, including gaining access to high-level accounts and to the code for the BA website. The attacker was then able to divert user traffic from the BA website so that customer payment card data were copied and redirected to the attacker's site without interrupting the usual BA booking and payment procedure, remaining undetected until a third party brought it to BA's attention.

The Penalty Notice issued by the ICO commenced with a much-reduced penalty of £30 million as an appropriate starting point before any mitigating factors were taken into consideration. No clear explanation is provided for such a significant reduction from the initial notice to fine, although it suggests it is likely that the ICO laid less blame on BA once the incident had been fully investigated.

THE BREACH

ICO investigators found that BA had failed under Articles 5(1)(f) and 32 of the GDPR to ensure appropriate security of the data. Specifically, there was a failure to use appropriate technical and organizational measures to protect against unauthorized or unlawful processing, and accidental loss, destruction or damage of personal data, that BA was responsible for as data controller. There were multiple weaknesses in BA's system that should have been identified and resolved, and had BA implemented one or more of the appropriate security measures available at the time, the attack could have been prevented, or its impact mitigated.

The Commissioner found that BA was processing a significant amount of personal data without appropriate security and it is unclear whether BA would have detected the data breach if the airline had not been alerted by a third party. The Commissioner also considered the severity of the data breach in terms of the high volume of data disclosed – an estimated 429,612 people were affected, with 185,000 customers having their payment card data compromised and 77,000 having their CVV numbers taken, the latter considered sensitive financial information and therefore high risk.

MITIGATING FACTORS

There were a number of mitigating factors, and as a result, the ICO further reduced the fine from £30 million to £20 million. Part of that reduction, £6 million, relates to mitigating factors specific to BA's response to the data breach. After becoming aware of the data breach, BA took immediate action to mitigate any damage suffered, promptly informed the ICO and affected data subjects of the breach in line with its reporting obligations, and cooperated fully with the Commissioner's enquiries. Additionally, the ICO accepted BA's argument that widespread reporting of the attack and the ICO's investigation had increased the awareness of other data controllers of the risks posed by cyberattacks. The ICO further accepted that the attention also had an adverse impact on BA's branding and reputation.

The ICO applied a further reduction of £4 million in light of the adverse financial impact of COVID-19 on BA's business and the wider aviation industry. This gives some indication of how the ICO will approach its duties over the coming months and suggests companies could expect fines to be reduced by roughly 10 percent to 15 percent, although the particular circumstances of the airline industry are not by any means universally felt, and it will remain to be seen whether this will be a common feature of GDPR fines issued during this period.

QUANTIFICATION METHODOLOGY

BA also submitted detailed representations in response to the method used by the ICO to reach the initial fine figure of £183.39 million. BA alleged that the Commissioner unlawfully applied an unpublished, turnover-centric quantification policy to calculate the initial fine. The Commissioner agreed that the draft internal procedure used should not have been relied on in the present case, and so it was not used in deciding the final penalty amount. This provides some relief to data controllers that a significant percentage of their global turnover will not automatically be at risk in the most serious breaches (which could lead to astronomical fines in large global groups).

However, the Commissioner is obliged to ensure penalties are "effective, proportionate, and dissuasive." Therefore, a data controller's turnover remains a relevant and important, but not necessarily a determining, factor.

WIDER IMPLICATIONS

Despite a huge reduction from the initial fine amount, £20 million remains the biggest fine ever issued by the ICO for a breach of GDPR and is a clear statement of the seriousness it places on data processing responsibilities. The ICO did not accept BA's suggestion that the airline industry should be subjected to a lower security standard compared with other industries, and while the ICO recognized that the breach was caused by a sophisticated cyberattack, this does not alter BA's obligations as a data controller to have in place adequate security measures.

A company the size of BA, that processes large amounts of high-risk data, is expected to be aware that it is a likely target of such an attack and must have up-to-date systems in place to protect data. This is a reminder to all businesses, given the increasing number of cyberattacks mounted during the COVID-19 pandemic, that data security remains paramount. While it may not be possible to prevent a cyberattack, having appropriate well-rehearsed internal response procedures, particularly in respect of breach notification and remediation measures, will certainly help soften the blow.