AN A.S. PRATT PUBLICATION
NOVEMBER-DECEMBER 2019
VOL. 5 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 NUMBER 9 NOVEMBER-DECEMBER 2019

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 [275] (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

(2019–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 inquiries 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.

Can a Security Breach Impact a Company Years Later? Lessons Learned from the Equifax Breach

By Stephen E. Reynolds and Rachel Spiker*

Security incidents continue to impact companies in a multitude of ways, and often the full impact of an incident is not realized until years after the breach. The authors of this article discuss lessons learned from the Equifax breach.

A breach of cybersecurity can cost a company millions of dollars[1] and now may even significantly lower its creditworthiness.[2] Two years after its massive data breach was announced, Equifax still faces serious fallout from the breach[3]—from damage to its professional reputation, to the fines paid to several federal organizations, and several lawsuits.[4] Moody's Investor Service ("Moody's") recently downgraded its rating of Equifax citing the company's cybersecurity issues as the reason. Security incidents continue to impact companies in a multitude of ways, and often the full impact of an incident is not realized until years after the breach.

THE 2017 EQUIFAX BREACH

Equifax, a major credit score bureau, was the victim of one of the largest cybersecurity breaches in history.[5] Beyond its credit report analytics, Equifax is known for purchasing and selling personal data.[6] Even those who may not have provided data directly to Equifax may still find their personal data in the hands of Equifax because

* Stephen E. Reynolds, a former computer programmer and IT analyst, is a partner in Ice Miller's Litigation Group and co-chair of the firm's Data Security and Privacy Practice. Rachel Spiker is an associate in firm's Data Security and Privacy and Litigation Groups who focuses much of her work on data breach and security incident response. The authors may be reached at stephen.reynolds@icemiller.com and rachel.spiker@icemiller.com, respectively. Summer associate Arqeil Shaw contributed to this article.

[1] Sydny Shepard, *The Average Cost of a Data Breach*, https://securitytoday.com/articles/2018/07/17/the-average-cost-of-a-data-breach.aspx (Jul 17, 2018).

[2] Kate Fazzini, Equifax just became the first company to have its outlook downgraded for cyber attack, https://www.cnbc.com (May 22, 2019).

[3] *Id.*

[4] Ben Lane, Equifax expecting punishment from CFPB and FTC over massive data breach, https://www.housingwire.com (Feb 25, 2019).

[5] Steve Symanovich, *Equifax Data Breach Affects Millions of Consumers. Here's What to Do.,* https://www.lifelock.com/learn-data-breaches-equifax-data-breach-2017.html (last visited Jun 25, 2019).

[6] Equifax, https://www.equifax.com/about-equifax/company-profile/ (last visited Jun 25, 2019).

Equifax obtains much of its content from third party companies.[7] Companies who have vast stores of personal data, like Equifax, are prime targets for cyberattacks.[8]

On September 7, 2017, Equifax announced it was breached.[9] Although the incident was reported in September, the unauthorized data collection process occurred from mid-May until July 29, 2017. Personal identifiable information, including names, social security numbers, birthdates, addresses, and driver's licenses numbers, were stolen. As a result, an estimated 148 million people were potentially impacted by the data breach.[10] Experts can only speculate to the full extent of the data stolen because the data itself is still missing. The personal data profiles were not affected uniformly—some individuals' addresses were stolen, while others lost social security information, date of birth, or other pieces of identifiable information.[11]

RESULTS OF EQUIFAX'S BREACH

Following the breach, the Federal Trade Commission ("FTC") and the Consumer Financial Protection Bureau ("CFPB") stated they plan to seek "injunctive relief damages."[12] Equifax is still being investigated by the District of Columbia, the Department of Justice, the Securities and Exchange Commission ("SEC"), certain Congressional Committees of the House of Representatives and Senate, the United Kingdom's Financial Conduct Authority, and the Office of the Privacy Commissioner of Canada.[13] Equifax also faces lawsuits from more than 1,000 individual consumers, a 50 states class action lawsuit, its own shareholders, and even the Indiana Attorney General.[14] The Indiana Attorney General filed a complaint[15] against Equifax on May 6, 2019 seeking civil penalties, consumer restitution, costs, and injunctive relief as a result of the massive data breach that compromised the personal information

[7] Bruce Schneier, *Don't waste your breath complaining to Equifax about data breach*, https://www.cnn.com (Sept. 11, 2018).

[8] *Id.*

[9] Symanovich, *supra* note 5.

[10] Merrit Kennedy, *Equifax Says 2.4 million More People Were Impacted by Huge 2017 Breach*, https://www.npr.org (Mar 1, 2018).

[11] *Id. See also* Kate Fazzini, *The great Equifax mystery: 17 months later, the stolen data has never been found, and experts are starting to suspect a spy scheme*, https://www.cnbc.com (Feb 13, 2019).

[12] Lane, *supra* note 4.

[13] *Id.*

[14] *Id. See also* Tara Swaminath, *Equifax now hit with a rare 50-state class-action lawsuit*, https://www.csoonline.com/article/3238076/equifax-now-hit-with-a-rare-50-state-class-action-lawsuit.html. (Nov 22, 2017); *see also*, *Equifax Hit With Indiana Lawsuit Over 2017 Data Breach*, https://news.bloomberglaw.com/privacy-and-data-security/equifax-hit-with-indiana-lawsuit-over-2017-data-breach, (May 6, 2019).

[15] http://src.bna.com/HWW.

of nearly 148 million Americans.[16] The Indiana Attorney General lawsuit alleges Equifax chose to increase revenue instead of protecting its consumers by improving security measures through logical opportunities.[17]

During its first quarter earnings release, Equifax revealed it expected to lose upwards of $700 million for "certain legal proceedings and investigations related to the 2017 cybersecurity incident."[18]

EQUIFAX'S LOWERED CREDIT RATING

Moody's has a longstanding history of providing creditable financial analytics.[19] Moody's ranks companies from Aaa to C (Aaa is the highest and C is the lowest), which determines the creditworthiness of borrowers. Moody's is currently integrating cybersecurity risk into its credit rating algorithms.[20] Equifax's outlook has been downgraded after a recent Moody's report on the topic.[21] Cybersecurity is a significant topic of importance for consumers and companies.[22] Equifax is the first company impacted by Moody's new cybersecurity considerations.[23]

Equifax's credit rating was downgraded due to the $700 million dollars in legal disputes and sanctions it is expected to pay.[24] Equifax plans to improve its cybersecurity with estimated expense costs and capital investments of more than $400 million dollars. This also played a role in its downgraded outlook.[25] It is likely that higher cybersecurity costs will continue to hurt Equifax's profit margins in the future according to Moody's.[26]

WHAT CAN MY COMPANY DO TO PLAN AND PREPARE?

1. Prepare a Cybersecurity Plan

The process of preparing a cybersecurity plan allows for a company to obtain a better picture of the technology being used by the company, what types of information the company is collecting and processing, how to best protect that data, and more.

---

[16] *AG Hill files suit against Equifax for 2017 data breach,* https://www.theindianalawyer.com/articles/50221-ag-hill-files-suit-against-equifax-for-2017-data-breach, (May 7, 2019).
[17] *Id.*
[18] *Id.*
[19] Moody's, https://www.moodys.com (last visited Jun 25, 2019).
[20] Fazzini, *supra* note 2.
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*

A review of the types of data a company collects and how that data is stored and processed is a good starting point. Involving oversight from multiple areas of the company to create the cybersecurity plan allows for all parties with a stake in the protection of the data to be involved. Involving parties outside of just the information technology ("IT") specialists allows for greater understanding of the reasons behind the policies and plan.

2. Obtain a Cyber Liability Insurance Policy

A cyber liability insurance policy has the potential to cover a multitude of losses such as liability for lost data; remediation costs for investigations, notifications and repairs to systems after a security incident; and settlement costs associated with a security incident. Typically, a cyber liability insurance policy will give a company access to experts who can assist with a security incident.

3. Provide Cybersecurity Training and Education to Employees

Providing employees with cybersecurity training is key; the first line of defense against a security incident is often people. By providing training and education about potential threats, best practices, and appropriate processes, a company can help to avoid incidents or attacks that are easily preventable.

4. Prepare an Incident Response Plan

A security incident occurs, your emails have been hacked, financial information has been compromised, now what? Creating an incident response plan will lay out the steps the company should take following an incident. The process of creating a plan helps to eliminate the stress and confusion that often surrounds a security incident by establishing the actions and processes before an incident occurs. A well-crafted incident response plan can have a significant impact on the amount of damage caused by an incident.

5. Perform Table Top Exercises

A tabletop exercise is an activity in which key personnel who are assigned management roles and responsibilities in the event of a security incident are gathered to discuss, in a non-threatening environment, various simulated security incident situations. The exercises are provided by third parties and allow key employees a chance to run through the company data security programs, policies, procedures, and other related processes. Tabletop exercises give employees the opportunity to become familiar with the plans in the event of a security incident and hopefully help to ensure the data security programs, policies, procedures, and other related processes are actually followed when an incident occurs.