IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

IN RE: MARRIOTT INTERNATIONAL, INC., CUSTOMER DATA SECURITY BREACH LITIGATION	MDL No. 19-md-2879 Judge Paul W. Grimm
This Document Relates To: CITY OF CHICAGO, Plaintiff, v. MARRIOTT INTERNATIONAL, INC., a Delaware corporation, and STARWOOD HOTELS & RESORTS WORLDWIDE, LLC, a Maryland limited liability company, Defendants.	This Document Relates to Case No. 8:19-cv-0654 **JURY TRIAL DEMANDED** **REDACTED VERSION**

FIRST AMENDED COMPLAINT

Plaintiff City of Chicago brings this First Amended Complaint against Defendants Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC (collectively referred to as "Marriott" unless otherwise indicated) to seek relief for harm and injuries arising from and as a result of the data breach that Marriott announced on November 30, 2018. Plaintiff, for its Complaint, alleges as follows:

INTRODUCTION

1. On November 30, 2018, the hotel conglomerate Marriott announced it had experienced what is now recognized as the second largest data breach in history.[1] Setting aside

[1] *Marriott Announces Starwood Guest Reservation Database Security Incident* (2018), Marriott International, http://news.marriott.com/2018/11/marriott-announces-starwood-guest-

that it waited over 80 days after first learning of the breach to inform the public, Marriott revealed that the data of over 500 million of its guests, including their names, mailing addresses, phone numbers, email addresses, birth dates, credit and debit card payment numbers and expiration dates, and even passport numbers, among other things, had been exposed to hackers *for the past four years*.

2. Marriott could and should have prevented the data breach by implementing and maintaining reasonable safeguards, consistent with the representations it made to the public in its marketing materials and privacy statements, and compliant with industry standards, best practices, and state law. Unfortunately, Marriott failed to do so.

3. An independent forensic investigation conducted after the breach was announced revealed [redacted]

- [redacted]
- [redacted]
- [redacted]

reservation-database-security-incident/ (last visited June 20, 2019).

2 [redacted]

3 [redacted]

[redacted] and

- [redacted]

4. As a result, attackers were able to gain virtually unfettered and unchecked access to Starwood's (Marriott's wholly-owned subsidiary's) systems and were able to freely copy and export hundreds of millions of its guests' highly sensitive and personal information, including from Starwood's guest reservation and room information database.

5. Each detail of this breach is alarming by itself, but what is even more egregious is Starwood reported a data breach in 2015 when it detected malware on its point of sale ("POS") systems in over 100 locations in North America. The investigation that began in November 2015, and concluded in January 2016, should have revealed this breach. Instead, it incorrectly found that the Starwood customer reservation database—the database at issue in this breach—had not been impacted.

6. Around this time, Marriott and Starwood also had a string of other data security incidents, including:

- A security researcher found a SQL injection[5] bug on a Starwood website, which was likely used to gain access to Starwood databases (and vulnerabilities like this were for sale on the Dark Web at the time);
- Marriott's Computer Incident Response Team was compromised and attackers gained access to their internal email accounts, as shown in Section

---

4 [redacted]

5 A "SQL injection" is a well-known security vulnerability where an attacker can force a database to execute a malicious query in order to view, modify, or delete information within the database.

III below;

- Security researcher Alex Holden discovered that six starwoodhotels.com domains were controlled by a Russian botnet[6];

- Starwood's cloud portals had an easily guessable password, which could allow hackers to access business and financial records, security controls, and booking information; and

- Shortly after Marriott announced this breach, *it was revealed that Marriott was still not properly protecting a wealth of information, including its own internal business, legal, and operational documents.* Specifically, records from Starwood's Global Records Center were cached by Google and were, therefore, publicly accessible online. Starwood described this system as containing confidential and proprietary information relating to property management, technology, vendors, mergers, and legal documents, among other things. Not only was this data sensitive as it applied to Defendants' own business practices, but it was likely a virtual treasure trove of exploitable information for gaining access to additional customer information. The threat posed by this vulnerability was real and ongoing after the breach announced on November 30, 2018 became public and yet was unknown to Defendants.

7. Ultimately, by failing to secure its guests' personal and sensitive data—despite its legal obligations to do so—Marriott has subjected Chicago residents whose personal information was in Starwood's guest reservation database ("Chicago Victims") to potential identity theft, financial fraud, tax return scams, and other potential ongoing harm. At the very least, Chicago Victims will be forced to spend time and money in an attempt to protect themselves against the substantially increased risk of injury caused by Marriott's misconduct.

8. While some security threats are unavoidable in a rapidly-developing technological environment, Marriott's failure to implement reasonable data security protocols fell far short of

[6] A "botnet" is a network of hijacked computers and devices infected with malware that allows them to be remotely controlled by a hacker. Botnets are often used to send spam, crack passwords, and launch Distributed Denial of Service attacks.

its promises and jeopardized hundreds of millions of its customers' sensitive personal information.

9. Accordingly, Plaintiff City of Chicago brings this suit to seek redress for Marriott's unlawful conduct. Plaintiff seeks civil penalties and all necessary, appropriate, and available equitable and injunctive relief to address, remedy, and prevent harm resulting from Marriott's misconduct.

PARTIES

10. Plaintiff City of Chicago is a municipal corporation and a home-rule unit organized and existing under the laws of the State of Illinois.[7]

11. Defendant Marriott International, Inc. is a Delaware corporation with its principal place of business in Bethesda, Maryland.

12. Defendant Starwood Hotels & Resorts Worldwide, LLC is a Maryland limited liability company with its principal place of business in Bethesda, Maryland.

JURISDICTION AND VENUE

13. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332 because the matter in controversy exceeds $75,000 and the City of Chicago is a citizen of a different State than Defendants.

14. This Court has personal jurisdiction over Defendants because they conduct significant business in this District and maintain their principal places of business in this District.

[7] Following an investigation, Rosa Escareno, Commissioner for the City of Chicago Department of Business Affairs and Consumer Protection, determined that Defendants engaged in practices prohibited by Section 2-25-090 of the Municipal Code of Chicago ("MCC"), and subsequently requested that the City of Chicago Department of Law bring legal action against Defendants seeking all available relief.

15. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendants reside in this District.

FACTUAL BACKGROUND

I. An Overview of Marriott.

17. Marriott is a leading global hotel chain, operating more than 7,000 properties across 131 countries. Directly or through its subsidiaries, Marriott operates approximately 33 hotels throughout the City of Chicago.

18. Marriott entered into a merger agreement with Starwood in 2015, completing the acquisition the following year. Since the Starwood acquisition, Marriott has become the world's largest hotel chain and now accounts for 1 out of every 15 hotel rooms around the globe.

19. Starwood operates hotels under brand names such as Sheraton Hotels & Resorts, Westin Hotels and Resorts, W Hotels, St. Regis, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Meridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels. Starwood also operates timeshare properties under the brands Sheraton Vacation Club, Westin Vacation Club, The Luxury Collection Residence Club, St. Regis Residence Club, and Vistana.

16. There were at least 10 Starwood Properties that operated in Chicago during the period covered by this data breach: Aloft Chicago Downtown River North, Aloft Chicago Mag Mile, Hotel Zachary, Sheraton Grand Chicago, The Gwen Hotel, The Robey Chicago, The Westin Chicago River North, The Westin Michigan Avenue Chicago, W Chicago - City Center, and W Chicago - Lakeshore.

17. Marriott is licensed to conduct business in the City of Chicago and obtained separate licenses to operate each of its hotels, serve food and liquor, maintain health clubs,

provide parking, and otherwise operate in Chicago. *See*, *e.g.*, MCC §§ 4-6-010(c), 4-6-180, *et seq*.

II. Marriott Collects Incredibly Sensitive Information From Its Customers.

20. In order to stay at a Marriott property, guests must first make a reservation and provide Marriott their full names, mailing addresses, email addresses, telephone numbers, credit or debit card numbers, travel itinerary, account data related to its customer-loyalty programs, and often times other sensitive information, like passport information. Marriott maintains this information in its guest-reservation databases.

21. According to the Privacy Statement posted on its website, Marriott also collects other "Personal Data" (which it defines as "data that identif[ies] you as an individual or relate to an identifiable individual") about its guests during the course of their visits, including their:

- Name
- Gender
- Postal address
- Telephone number
- Email address
- Credit and debit card number or other payment data
- Financial information in limited circumstances
- Language preference
- Date and place of birth
- Nationality, passport, visa or other government-issued identification data
- Important dates, such as birthdays, anniversaries and special occasions
- Membership or loyalty program data (including co-branded payment cards and/or travel partner program affiliations)
- Employer details
- Travel itinerary, tour group or activity data
- Prior guest stays or interactions, goods and services purchased, special service and amenity requests
- Geolocation information
- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts.

22. In more limited circumstances, Marriott also collects:

- Data about family members and companions, such as names and ages of children
- Biometric data, such as digital images
- Images and video and audio data via: (a) security cameras located in public areas, such as hallways and lobbies, in its properties; and (b) body-worn cameras carried by its loss prevention officers and other security personnel
- Guest preferences and personalized data ("Personal Preferences"), such as customers' interests, activities, hobbies, food and beverage choices, services and amenities of which customers advise Marriott or which it learns about during customers' visits.

23. In fact, Marriott collects and uses such detailed and sensitive consumer data that it enlisted a leading data analytics company to use that wealth of data to identify, attract, and retain the most profitable customers. In other words, Marriott uses data it collects to help predict and influence its customers' future behaviors (*i.e.*, convincing them to stay at their properties). According to the analytics company, that's because there's no lack of available data here. Together, they have access to household profiles, including number of kids, type of jobs held by family members, their salaries, where and how they spend their money, and even the type of jeans they buy. The level and granularity of data Marriott and this analytics company collects is frightening. They can even identify when a guest leaves a hotel, where they go, and when they're at home and in bed for the night (by tracking their cell phone's location and activity).

24. Recognizing that consumers value companies that keep their information private and secure, Marriott represents to its guests—including Chicago residents—that it uses "reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information."[8]

[8] *Marriott U.S. Privacy Shield Guest Privacy Policy*, Marriott, https://www.marriott.com/about/global-privacy.mi.

III. Marriott Has a Significant History of Failing to Adequately Protect Sensitive Personal Information.

25. Criminal hackers have repeatedly exploited vulnerabilities in corporate security to obtain personal information about consumers. Over the last decade, the press has catalogued massive data breaches at companies like Equifax, Uber, and Yahoo.[9] These data breaches have also been the subject of well-publicized governmental investigations.

26. According to cybersecurity experts, "hotels are . . . [particularly] attractive target[s] for hackers because they hold a lot of sensitive information, including credit card and passport details, but often don't have security standards as tough as those of more regulated industries."[10] Not surprisingly, many of Marriott's competitors—like Hilton, Holiday Inn, and Hyatt—have had significant data breaches in recent years.[11]

27. These alarming trends and targeting of the hospitality industry in particular should have put the world's leading hotel chain on notice that it was a prime target for an attack. Unfortunately, Marriott did not and, historically, has not taken that threat seriously—Marriott has a significant history of failing to adequately protect its own computer networks.

28. For example, in 2014, a security researcher found a SQL injection bug (*i.e.*, a vulnerability in a website that an attacker with basic hacking skills can exploit to access a

---

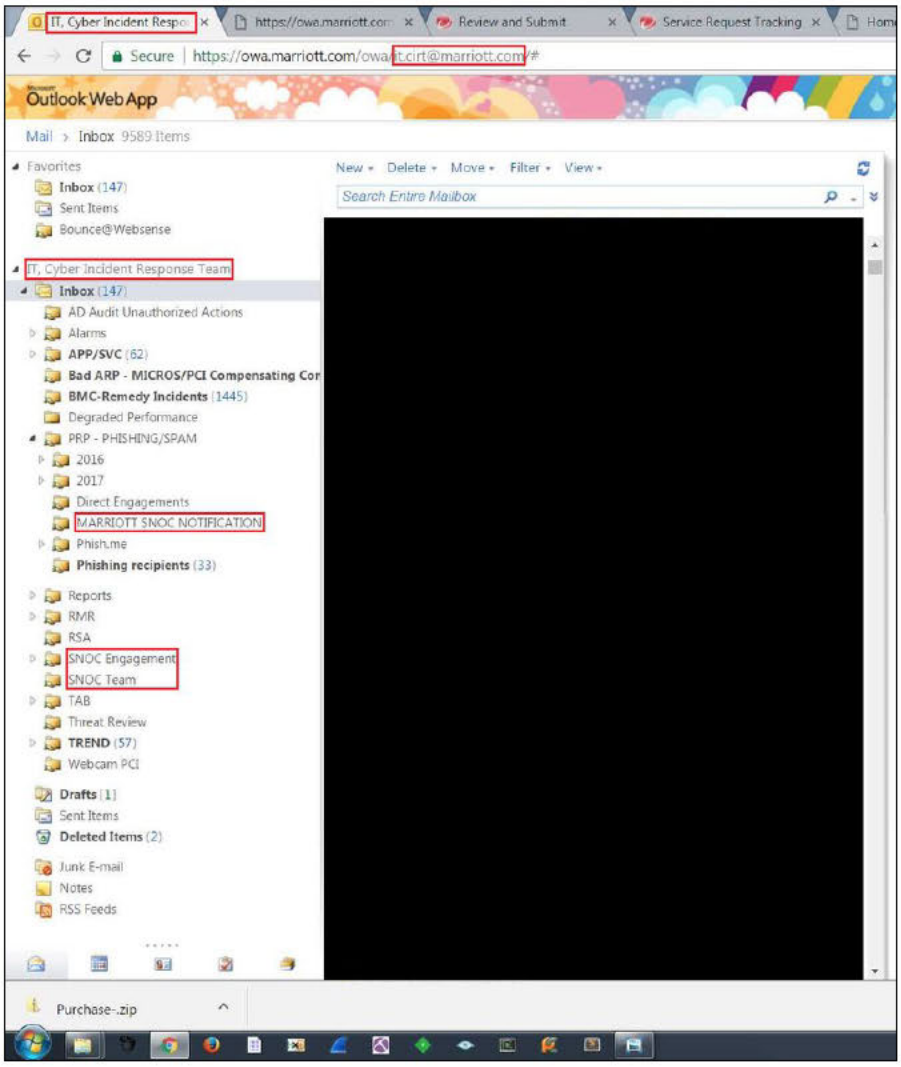
[9] Taylor Armerding, *The 17 Biggest Data Breaches of the 21st Century*, CSO Online (Dec. 20, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

[10] *Breach Puts Hotel Guests' Data at Risk*, Arkansas Democrat Gazette (Dec. 1, 2018), https://www.arkansasonline.com/news/2018/dec/01/breach-puts-hotel-guests-data-at-risk-2/.

[11] *Marriott: Data on 500 Million Guests Stolen in 4-Year Breach*, Krebs on Security (Nov. 30, 2018), https://krebsonsecurity.com/2018/11/marriott-data-on-500-million-guests-stolen-in-4-year-breach/.

database) that likely was used to gain access to Starwood databases. In fact, at the time, vulnerabilities like this were for sale on the Dark Web.

29. Later, Marriott's Computer Incident Response Team ("CIRT") was compromised due to an external analyst downloading a malware sample, which executed and provided attackers access to the CIRT's email accounts. Figure 1 shows a screenshot—recovered from a Nigerian hacker's server—of Marriott's CIRT teams email inbox.[12]



(**Fig. 1.**)

12 MalwareHunterTeam (@malwarehunterteam), Twitter (July 1, 2017, 2:57 AM), https://twitter.com/malwrhunterteam/status/881089396124078080.

30. In another example, security researcher Alex Holden had discovered that six servers hosting starwoodhotels.com domains were controlled by a Russian botnet (*i.e.*, a network of private computers infected with malicious software and controlled as a group without the owner's knowledge). Holden had also discovered that one of Starwood's cloud portals had an easily guessable password, which could allow hackers to access business financial records, security control, and booking information.

31. It should be no surprise then that on November 20, 2015—shortly after Marriott announced its acquisition of Starwood—Starwood announced the discovery of malware that has been installed on POS systems at a number of its hotels in North America. The malware affected Starwood's various restaurants, gift shops, and other payment processing centers at over 50 locations in North America.[13]

32. The malware collected customer's payment card information from Starwood's POS systems, including the cardholder's name, card number, security code, and expiration date.[14]

33. After the discovery of the malware in 2015, Starwood employed a third-party forensic team of experts to conduct an "extensive investigation" to determine the source of the malware and the extent of its impact. Months after the initial discovery, Starwood updated its customers (in January 2016) about the details of the breach. Starwood also released a comprehensive list of all hotels and resorts affected by the malware, which doubled from over 50 to 100 impacted locations.

---

13 *Letter From Our President*, Starwood Hotels and Resorts (Nov. 20, 2015), *available at* https://oag.ca.gov/system/files/starwood-notice-materials_0.pdf.

14 *Id*.

34. In an effort to "comfort" its customers and keep them coming back to its properties, Starwood (incorrectly) informed them that its guest reservation databases were not impacted.

35. Unfortunately, Marriott failed to discover then that hackers actually had on-going access to Starwood's guest reservation database.

IV. Marriott Failed to Detect A Four-Year Long Breach of Its Reservation Database and Then Waited Over 80 Days to Notify Chicagoans.

36. On November 30, 2018, Marriott revealed that its Starwood reservation database had been hacked. The Starwood reservation database contained information pertaining to customers that stayed at Starwood properties like the Sheraton, W Hotels, Westin, and St. Regis, among many others.

37. Marriott explained that it first learned about the data breach on September 8, 2018, when a Marriott administrator received an alert from an "internal security tool" that someone attempted to access the Starwood guest reservation database. Marriott then "engaged leading security experts to help determine what occurred."[15]

38. The security experts' findings were shocking. They learned that the breached database contained information on approximately 500 million guests who made a reservation at a Starwood property.

39. For approximately 327 million of its guests, the compromised information included a combination of the guests':

- full name;
- mailing address;
- phone number;
- email address;

[15] *Starwood Guest Reservation Database Security Incident*, Kroll, https://info.starwoodhotels.com/ (last visited June 20, 2019).

- passport number;
- Starwood Preferred Guest account information;
- date of birth;
- gender;
- arrival and departure information;
- reservation date; and
- communication preferences.[16]

40. The remaining guests likely had their names and email addresses taken.

41. Defendants could have attempted to protect this information by encrypting it but, on information and belief, largely failed to do so. Indeed, Marriott admitted that "approximately 5.25 million unencrypted passport numbers were included in the information accessed by an unauthorized third party."[17]

42. The size of Marriott's data breach is the second largest in history and the largest since Yahoo's 2013 data breach affecting 3 billion individuals.[18]

43. Marriott also revealed that the breached database included approximately 8.6 million of its guests' encrypted payment card numbers and the card expiration dates. Although Marriott claims the card numbers were encrypted by using Advanced Encryption Standard encryption (AES-128), certain evidence may be missing, so it has not ruled out the possibility that the two components needed to decrypt payment card numbers have also been accessed. In other words, in another egregious example of its substandard security practices, it may have been possible for hackers to have obtained the necessary keys or passwords to decrypt customers' payment card numbers.

---

16 *Id.*

17 *Marriott Provides Update on Starwood Database Security Incident*, Marriott International (Jan. 4, 2019), https://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/.

18 Nicholas Rivero, *The Biggest Data Breaches Of All Time, Ranked*, Quartz (Nov. 30, 2018), https://qz.com/1480809/the-biggest-data-breaches-of-all-time-ranked/.

V. Marriott Botched Its Response to the Data Breach.

44. Marriott claims to have discovered the data breach on September 8, 2018, but then waited 83 days (until November 30, 2018) to inform the public and its guests. That delay was unreasonable and prevented Chicago Victims from taking steps to protect their personal information.

45. To make matters worse, Marriott made two critical mistakes when it finally notified Chicago Victims. First, Marriott emailed Chicago Victims from the address "email-marriott.com." That address is registered to a third party, and cybersecurity experts noted that "there was little else to suggest the email was at all legitimate."

46. Second, as one cybersecurity expert observed, the email address "email-marriott.com" is "easily spoofable."[19] The Federal Trade Commission warned consumers victimized by the Data Breach that "scammers try to take advantage of situations like this" by "send[ing] emails with links to fake websites to try to trick people into sharing their personal information."[20] A press report noted that Marriott's use of the address "email-marriott.com" is so "problematic" that "security experts are filling in the gaps—at their own expense"—by registering similar addresses such as "email-marriot.com" and "email-mariott.com" to educate victims and "make sure that scammers didn't register the domains themselves."[21]

47. Beyond its flawed efforts to notify Chicago Victims, Marriott established a

---

19 Zack Whittaker, *Marriott's breach response is so bad, security experts are filling in the gaps — at their own expense*, TechCrunch, *available at* https://techcrunch.com/2018/12/03/marriott-data-breach-response-risk-phishing/ (last visited June 20, 2019).

20 Seena Gressin, *The Marriott data breach*, Federal Trade Commission Consumer Information (Dec. 4, 2018), https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach.

21 Whittaker, *supra* n.19.

website to address questions about the Data Breach. Marriott failed in this task too: the website had problems "staying online."

VI. [redacted].

48. [redacted]

49. [redacted]

50. [redacted]

51. [redacted]

[redacted]	[redacted]
[redacted]	[redacted]

	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

52. [redacted]

[redacted]:

- [redacted]
- [redacted]

22 [redacted]

- [redacted]
- [redacted]
- [redacted]

53. Had Marriott implemented any one of the security measures described above, it could have prevented (or significantly reduced the damage) of the breach.

VII. Chicago Victims Have Already Suffered Significant and Lasting Harm as a Result of Marriott's Misconduct.

54. Though the City of Chicago need not allege injury or causation to state a claim for violations of the Municipal Code of Chicago, Marriott's misconduct has injured Chicago residents, who make reservations at Marriott properties from Chicago and stay in Marriott's Chicago hotels and throughout the country.

55. First, consumers place value in data privacy and security, and they consider that when making purchasing decisions. In fact, it is widely accepted that consumers are willing to pay higher prices to do business with merchants that better protect their privacy and information. A number of studies have found that U.S. consumers consider security when purchasing goods and services, and that approximately 50% of consumers would consider paying more to work with a company with better security.[24] Likewise, studies have shown that over 70% of U.S.

---

23 [redacted]

24 *Beyond the Bottom Line: The Real Cost of Data Breaches*, FireEye, https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf?mkt_tok=eyJpIjoiTW1FMFpqTTBNekU0WkRrdyIsInQiOiJHZjEza3huK1Rnb

consumers will provide less personally identifiable information to organizations that suffer a data breach.[25]

56. Consumer technology markets have likewise demonstrated that consumers value their privacy and security and incorporate data security practices into their purchases. For example, companies have begun providing consumers with "cloaking services" that allow them to browse the Internet anonymously for a fee. Likewise, companies now offer services that, in exchange for a monthly fee, will offer online services designed to protect data privacy.

57. Because of the value consumers place on data privacy and security, services with better security practices command higher prices than those without. Indeed, if consumers did not value their data security and privacy, profit-seeking corporations (like Marriott) would have no reason to tout their privacy and security credentials to current and prospective customers.

58. These value propositions reflect the fact that consumers view companies that promise to adequately secure customer data as being far more useful—and valuable—than those with substandard protections.

59. As a result, a hotel service with substandard data security and privacy protections is less useful and valuable than a product or service using adequate security protocols, and is, in reality, a different service entirely.

60. Stated simply, had consumers known the truth about Marriott's data security practices—*e.g.*, that it did not adequately protect and store their data—they would not have purchased rooms or otherwise stayed at Marriott hotels.

WswajYyT2R5RDNEZStsUzQ5ZWFtVTZaOVZUNTdaRXZJdGRnaHE1SnJ3WWIxbDhuNUVaeFdFakpJVlE0MStZc2FUeDlIbFV1NTJEcys1OUo4a1NGelZcL3JhRjlZcWxQNkV6a3hNZ2xqK1ZSMEI4bUY1MWNHMk0ifQ%3D%3D (last visited June 20, 2019).

[25] *Id.*

61. Second, Marriott customers have already suffered significant and lasting harm as a result of the data breach, and such harm is likely to continue and worsen over time.

62. Armed with an individual's sensitive and personal information—like names, mailing addresses, email addresses, phone numbers, passport numbers, dates of birth, and travel information—hackers and criminals can commit identity theft, financial fraud, and other identity-related crimes.

63. Identity theft results in real financial losses, lost time, and aggravation to consumers. In fact, in its 2014 Victims of Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of all identity theft victims never had those losses reimbursed.[26] The average out-of-pocket loss for those victims was $2,895.

64. Identity theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings."[27] The report also noted that more than one-third of identity theft victims suffered moderate or severe emotional distress due to the crime.[28]

65. Chicago Victims are also subject to a substantially increased risk of injuries unique to this data breach:

- "[M]any experts and government officials have expressed concern that the passport numbers" taken in the data breach, "in concert with the other

---

26 *See* Erika Harrell, *Victims of Identify Theft*, 2014, U.S. Dept. of Justice, Bureau of Justice Statistics, at 6 & Table 6, https://www.bjs.gov/content/pub/pdf/vit14.pdf (last updated Nov. 13, 2017).

27 *Id*. at 8.

28 *See id.* at 9, Table 9.

personal data compromised by the hack, could pose serious risks of identity theft—and be a threat to national security."[29]

- Criminals can steal "reward points" that guests accumulated under Starwood's customer-loyalty program. Experts have called it "easy" for hackers to redeem points for gift cards, making loyalty-account information far more valuable than social-security numbers on the black market.[30]

66. At the very least, Marriott's conduct has and/or will require Chicago Victims to spend time and money in an attempt to prevent identity theft and financial fraud. The Federal Trade Commission suggested that victims of the data breach obtain and review their credit reports for signs of identity theft, carefully review their payment-card account statements, place fraud alerts on credit files, and consider placing credit freezes on credit reports.[31] Marriott's conduct therefore will impose burdens on Chicago Victims for years to come.

67. Ultimately Marriott's misconduct has substantially increased the risk that the affected Marriott customers will be, or already have become, victims of identity theft or financial fraud.

VIII. The Relief Offered by Marriott is Inadequate.

68. Marriott's proposed remedies for victims of the data breach fall short.

69. Marriott initially offered only the opportunity to enroll in a one-year free subscription to a service called WebWatcher, which monitors internet sites where personal

---

[29] Taylor Telford, *Marriott will pay for new passports after data breach 'if fraud has taken place'*, The Washington Post (Dec. 4, 2018), https://www.washingtonpost.com/business/2018/12/04/marriott-will-pay-new-passports-after-data-breach-if-fraud-has-taken-place/?utm_term=.b6aa4acaedf4.

[30] Jennifer Surane & Katherine Chiglinsky, *All Those Starwood Points You Racked Up at Risk in Marriott Hack*, Bloomberg (Nov. 30, 2018), https://www.bloomberg.com/news/articles/2018-11-30/all-those-starwood-points-you-racked-up-at-risk-in-marriott-hack.

[31] Gressin, *supra* n.20.

information is shared and alerts consumers if their personal information is found. That offer suffers from several problems.

70. For example, WebWatcher does not alert consumers when new accounts have been opened in their names. Plus, as one cybersecurity expert stated, products (like WebWatcher) that monitor the dark-web "aren't particularly effective at protecting your data."[32]

71. In addition, identity thieves may simply wait until Marriott's one-year offer expires. Cybersecurity experts say that "identity thieves often wait to use the stolen data."[33] "Waiting gives thieves time to collect additional information and build out more robust identity profiles in order to open up credit cards in individual's names, file fraudulent tax returns, or get access to current bank accounts."[34] The U.S. Government Accountability Office similarly explained:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[35]

72. After public officials criticized Marriott's initial response, Marriott suggested that it may reimburse victims for the cost of obtaining new passports if Marriott "determines that

---

32 Octavia Blanco, *Why Marriott's ID Theft Protection May Not Be Enough*, Consumer Reports (Dec. 7, 2018) available at https://www.consumerreports.org/identity-theft/why-marriotts-id-theft-protection-may-not-be-enough/.

33 *Id.*

34 Matt Tatham, *A Year After the Equifax Breach: Are You Protecting Your Data?*, Experian, https://www.experian.com/blogs/ask-experian/a-year-after-the-equifax-breach-are-you-protecting-your-data/ (last visited June 20, 2019).

35 *Personal Information*, United States Government Accountability Office (June 2007), at 29, http://www.gao.gov/new.items/d07737.pdf.

fraud has taken place."[36] This suggestion is also inadequate. Some identity-theft experts recommend that victims of the Data Breach "consider renewing their passports" now, without waiting for identity thieves to act.[37] Victims who follow this advice will be unable to show that "fraud has taken place" and thus will be on the hook for the full $110 cost to renew a passport.

IX. Poor Security Practices Lead to Irreparable Harm.

73. Loss of sensitive personal information is no trivial matter. The consequences of stolen information and potential subsequent identity theft are so severe that the FTC recommends consumers shred documents containing sensitive data to protect themselves.

74. Some victims of identity theft lose access to their own money, see their tax refunds stolen, find it difficult or impossible to obtain credit, or face other financial woes. One identity theft victim found himself arrested at his home in Georgia and extradited to face trial for check fraud in Missouri before authorities were able to ascertain that they had indicted the wrong person.[38]

75. Once a consumer's personal information has been stolen, the risk of these adverse consequences is markedly higher, and it cannot be entirely eliminated. As a result of a data breach, it is reasonably probable that affected consumers will suffer identity theft in the future.

---

36 Robert Hackett, *Marriott Says It Will Pay for Replacement Passports After Data Breach. Here's Why That's Likely Baloney*, Fortune (Dec. 8, 2018), http://fortune.com/2018/12/08/marriott-breach-hack-starwood-passport-pay/.

37 Blanco, *supra* n.32.

38 *Identity Theft Victim Spends 32 Days in Missouri Jail*, WSB-TV (March 24, 2015), http://www.wsbtv.com/news/news/local/identity-theft-victim-spends-32-days-missouri-jail/nkdwW/.

76. The FTC recommends that consumers take a number of proactive steps when their personal information is compromised in a data breach, including filing taxes early, placing a credit freeze on their names, and frequently checking their credit reports.

77. The FTC also has recommendations for what consumers should do after someone begins using their information fraudulently. Many of these steps are complicated and require interactions with multiple government offices and private companies. Often, they require consumers to produce originals of documents that may be difficult to obtain, especially after identity theft has occurred. In some cases, the FTC recommends seeking legal counsel.[39]

78. Even following the FTC's recommendations is not enough. A single customer, monitoring her own credit, has no way to know when other affected consumers' contemporaneously stolen data begins surfacing on criminal marketplaces and starts being used for fraudulent purposes. That is a vital warning signal that would allow consumers to act quickly to protect themselves and prevent future (and, potentially, irreparable) harm.

79. Accordingly—and like the effect of a medical surveillance program established on behalf of groups of individuals exposed to asbestos—more sophisticated surveillance maintained on behalf of a larger group of individuals and operated by a government can alert consumers when, based on reported fraud and other indicators, they need to take immediate action to protect their credit.

COUNT 1
Unfair Practice—Failure to Safeguard Personal Information in Violation of MCC § 2-25-090(a)

80. Chicago incorporates all preceding allegations as if they were set forth herein.

---

[39] *When Information is Lost or Exposed*, Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/info-lost-or-stolen (last visited June 20, 2019).

81. The MCC provides: "No person shall engage in any act of consumer fraud, unfair method of competition, or deceptive practice while conducting any trade or business in the city. Any conduct constituting an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act … shall be a violation of this section." MCC § 2-25-090(a).

82. The Illinois Consumer Fraud and Deceptive Business Practices Act declares "unfair or deceptive acts or practices … in the conduct of any trade or commerce" to be "unlawful," regardless of "whether any person has in fact been … damaged thereby." 815 ILCS 505/2.

83. While conducting trade or commerce in Chicago, Marriott engaged in unfair acts or practices by failing to protect Chicago residents' personal information.

84. While conducting trade or commerce in Chicago, Marriott engaged in unfair acts or practices by failing to detect the data breach promptly.

85. While conducting trade or commerce in Chicago, Marriott engaged in unfair acts by inadequately responding to the data breach.

86. Marriott was aware of the risk of a data breach but, on information and belief, failed to implement reasonable safeguards that would have prevented the data breach, detected it sooner, and mitigated its effects.

87. Marriott's conduct offends public policy; is immoral, unethical, oppressive, and unscrupulous; and causes substantial injury to consumers.

88. Marriott's conduct independently violates MCC § 2-25-090(a). In addition, Marriott's violations of the Illinois Consumer Fraud and Deceptive Business Practices Act constitute violations of MCC § 2-25-090(a).

COUNT 2
Unlawful Practice—Failure to Implement and Maintain Reasonable Security Measures in Violation of MCC § 2-25-090(a)

89. Chicago incorporates all preceding allegations as if they were set forth herein.

90. The MCC provides that an "unlawful practice" under the Illinois Consumer Fraud and Deceptive Business Practices Act "shall be a violation of this section." MCC § 2-25-090(a).

91. The Illinois Consumer Fraud and Deceptive Business Practices Act provides: "Any person who knowingly violates . . . the Personal Information Protection Act . . . commits an unlawful practice within the meaning of this Act." 815 ILCS 505/2Z; *accord* 815 ILCS 530/20.

92. Accordingly, a knowing violation of the Illinois Personal Information Protection Act is also a violation of MCC § 2-25-090(a).

93. Section 45 of the Illinois Personal Information Protection Act states: "A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 ILCS 530/45(a).

94. Defendants are "data collectors" under the Illinois Personal Information Protection Act because Marriott and Starwood are "corporations" that "handle[], collect[], disseminate[], or otherwise deal[] with nonpublic personal information." *Id.* § 5.

95. Defendants violated Section 45 of the Illinois Personal Information Protection Act by failing to implement and maintain reasonable security measures to protect records that contain personal information concerning Chicago residents from unauthorized access, acquisition, destruction, use, modification, or disclosure.

96. Defendants' violations of Section 45 of the Illinois Personal Information Protection Act constitute violations of MCC § 2-25-090(a).

COUNT 3
Deceptive Practice—Misrepresentations and Material Omissions in Violation of MCC § 2-25-090(a)

97. Chicago incorporates all preceding allegations as if they were set forth herein.

98. The MCC prohibits any "deceptive practice while conducting any trade or business in the city. Any conduct constituting an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act . . . shall be a violation of this section." MCC § 2-25-090(a).

99. The Illinois Consumer Fraud and Deceptive Business Practices Act provides: "deceptive acts or practices, including but not limited to the use or employment of any deception fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in Section 2 of the 'Uniform Deceptive Trade Practices Act' … in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby." 815 ILCS 505/2.

100. While engaged in trade or commerce in Chicago, Marriott engaged in deceptive acts and practices by representing that Marriott used "reasonable" safeguards to protect Chicago residents' personal information.

101. While engaged in trade or commerce in Chicago, Marriott engaged in deceptive acts and practices by failing to disclose that Marriott lacked reasonable safeguards to protect Chicago residents' personal information.

102. Marriott intended that the public, including Chicago residents, rely on Marriott's deceptive representations and material omissions regarding the security of the personal information stored in Starwood's guest-reservation database.

103. Marriott's representations and omissions were deceptive because it did not maintain reasonable safeguards to protect Chicago residents' personal information.

104. Marriott's conduct independently violates MCC § 2-25-090(a). In addition, Marriott's violations of the Illinois Consumer Fraud and Deceptive Business Practices Act constitute violations of MCC § 2-25-090(a).

COUNT 4
Unlawful Practice—Failure to Give Prompt Notice of Data Breach in Violation of MCC § 2-25-090(a)

105. Chicago incorporates all preceding allegations as if they were set forth herein.

106. Section 10 of the Illinois Personal Information Protection Act provides: "Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system." 815 ILCS 530/10(a).

107. Marriott violated Section 10 of the Illinois Personal Information Protection Act by failing to notify Chicago Victims about the data breach in the most expedient time possible and without unreasonable delay.

108. Marriott's violations of Section 10 of the Illinois Personal Information Protection Act constitute violations of MCC § 2-25-090(a).

REQUEST FOR RELIEF

Plaintiff City of Chicago respectfully requests that the Court enter an order granting the following relief:

A. A declaration that Defendants violated MCC § 2-25-090(a). *See* MCC § 2-25-090(f)(4) (authorizing "an action for injunctive relief");

B. An injunction requiring Defendants to adopt and implement reasonable safeguards to prevent, detect, and mitigate the effects of data breaches. *See id.*;

C. A monetary fine awarded to Chicago. *See id* § 2-25-090(g) (stating that any person who violates any of the requirements of this section shall be subject to a fine of up to $10,000.00 for each offense, and that each day a violation continues constitutes "a separate and distinct offense to which a separate fine shall apply.");

D. The creation of a fund in the amount required to pay for adequate monitoring of this data breach, as well as for all precautions now necessary as a result of Defendants' conduct;

E. Attorneys' fees and costs awarded to Chicago;

F. Pre- and post-judgment interest awarded to Chicago; and

G. Any other relief that the Court deems reasonable.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can so be tried.

Respectfully submitted,

MARK A. FLESSNER
Corporation Counsel of the City of Chicago,

Dated: June 20, 2019

By: /s/ Stephen J. Kane

Stephen J. Kane
Acting Deputy Corporation Counsel
stephen.kane@cityofchicago.org

CITY OF CHICAGO DEPARTMENT OF LAW
Affirmative Litigation Division
121 North LaSalle Street, Room 600
Chicago, Illinois 60602
Tel: 312.744.6934
Fax: 312.744.5185

Dated: June 20, 2019

By: /s/ Benjamin H. Richman

Jay Edelson
jedelson@edelson.com
Benjamin H. Richman
brichman@edelson.com
Christopher L. Dore
cdore@edelson.com
David I. Mindell
dmindell@edelson.com
Sydney M. Janzen
sjanzen@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378