



Carol C. Villegas
Partner
212 907 0824 direct
212 907 0700 main
212 883 7524 fax
cvillegas@labaton.com

July 24, 2019

VIA ECF

Honorable Paul W. Grimm
United States District Court
District of Maryland
6500 Cherrywood Lane, Suite 465A
Greenbelt, MD 20770

New York Office
140 Broadway
New York, NY 10005

Re: *In re Marriott International Customer Data Security Breach Litigation*, No. 19-md-2879

Dear Judge Grimm:

We represent the Lead Plaintiff in the Securities Track, and along with plaintiffs in the Derivative Track (together, the “Securities Plaintiffs”), we submit this letter pursuant to the Court’s Order dated July 16, 2019 (ECF No. 334) and Case Management Order (“CMO”) No. 3 (ECF No. 279). In CMO 3, the Court allowed the Securities Plaintiffs to file a motion to unseal redacted portions of any complaint filed before this Court, seven days after the filing of the Consumer Complaint. (ECF No. 346). In the July 16, 2019 Order, the Court ordered that any party seeking to file a motion shall first submit a letter, no longer than three pages, stating the facts and bases supporting such relief. The Securities Plaintiffs intend to file the motion to unseal on July 29, 2019, and the bases for said motion along with a concise summary of the factual and legal support for the motion are contained herein.

Procedural Summary

The Government Track, (ECF Nos. 294, 296, & 298), Financial Institution Track, (ECF Nos. 306 & 328), and Consumer Track, (ECF No. 346), have each filed amended complaints, and have moved to file portions of those complaints under seal. (ECF Nos. 295, 307, & 345). On July 15, 2019, Defendants filed their motion to dismiss the Government Action complaint, attaching and relying on a copy of its investigation into the data breach – the Payment Card Industry Forensic Investigative Report (“PFI Report”), and also moved to file their memorandum under seal. (ECF Nos. 331 & 332). The Court provisionally granted these motions. (ECF Nos. 300, 314, 338, & 347). The Securities Plaintiffs seek to have all of these judicial records unsealed.

Factual Summary

The primary focus of the various complaints (and motion to dismiss) filed in the above-captioned coordinated action (the “Action”) is the second largest data breach in history at the largest hotel operator in the world (the “Breach”). The personal data of more than 380 million of Marriott’s guests was stolen. That information included names, addresses, payment card numbers, and passport numbers. There is a strong public interest in learning how the Breach occurred, why Marriott failed to discover the Breach during its due diligence in acquiring Starwood Hotels and Resorts Worldwide, LLC (“Starwood”), and how Marriott operated a guest reservation database for just shy of two years without discovering the Breach. Information relevant to each of these questions is contained in the PFI Report referenced in (but redacted from) the complaints and motion to dismiss.

Hon. Paul W. Grimm
July 24, 2019

Legal Basis for Unsealing

It is settled law that the First Amendment and common law protect the public's access to judicial records.¹ See *Virginia Dep't of State Police v. Washington Post*, 386 F.3d 567, 575 (4th Cir. 2004). In order to overcome either the common law or First Amendment presumption of access, the party seeking to keep the information from the public must at least provide "specific and concrete" concerns to warrant sealing or redactions. *Smith v. Westminster Mgmt., LLC*, 2018 WL 572867, at *5 (D. Md. Jan. 26, 2018). Merely attempting to avoid embarrassment, legal liability, or a harm to future business prospects are insufficient reasons under either standard to justify keeping information in judicial records from the public. See *id.* at *4. The party seeking the sealing must overcome the interest of the general public, which includes the financial markets as Marriott is a publicly traded company. *Minter v. Wells Fargo Bank, N.A.*, 258 F.R.D. 118, 124 (D. Md. 2009) (holding "[l]awsuits and their conduct are of interest to Main Street and Wall Street"). Under the First Amendment protection, the party seeking to seal materials must articulate a "compelling government interest" and explain how any redactions are narrowly tailored to serve that interest. *Rushford v. New Yorker Magazine, Inc.*, 846 F.2d 249, 253 (4th Cir. 1988).

The test for determining whether a First Amendment right of access is available is: 1) "whether the place and process have historically been open to the press and general public," and 2) "whether public access plays a significant positive role in the functioning of the particular process in question." *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 64 (4th Cir. 1989). On the first factor, records filed in judicial proceedings "have been historically open to both the press and the public." *Brown v. Lorings*, 2014 WL 6687120, at *3 (D. Md. Nov. 25, 2014). Additionally, the District of Maryland has held that the "already strong presumption of access is further strengthened when a document directly affects an adjudication, such as a complaint in a motion to dismiss proceeding." *Knight v. Mfrs. & Traders Tr. Co.*, 84 F. Supp. 3d 436, 446 (D. Md. 2015) (denying plaintiffs' motion to seal an amended complaint pursuant to confidentiality and protective orders). As to the second factor, "access to judicial records plays a positive role by ensuring transparency in the court system." *Brown*, 2014 WL 6687120, at *3.

Under the District of Maryland common law, which applies to all judicial records, in order to rebut the presumption of access, the party seeking to seal or redact a document must show "significant" individual interests that "heavily outweigh the public interests in access." *Washington Post*, 386 F.3d at 575. Regardless of whether the presumptive right of access is protected by the First Amendment or arises under common law, it "may be abrogated only in unusual circumstances." *Id.* at 576. Courts may grant motions to seal to protect sensitive personal information, such as detailed medical records, or trade secrets. *Minter*, 258 F.R.D. at 122-23. In weighing the public interest against the interests asserted by a party seeking to seal or redact, courts consider several factors, including (1) whether the records are sought for an improper purpose; (2) whether release would enhance public understanding of an important historical event; and (3) whether the public already has access to the information contained in the records. *Washington Post*, 386 F.3d at 575.

¹ A document is considered a "judicial record" if it "will play a role in the decisionmaking process of the Court." *Smith*, 2018 WL 572867, at *4.

**Labaton
Sucharow**

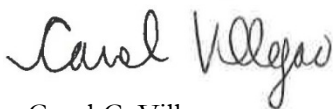
Hon. Paul W. Grimm
July 24, 2019

As an initial matter, these materials are clearly a matter of public interest to investors, consumers, and the American public. To underscore this, the Senate Committee on Homeland Security and Government Affairs held a **public** hearing to discuss these issues, and numerous national (and even international) news sources and financial analysts have covered the details of the data breach and have questioned why and how the breach happened, and why it took so long to discover.

The Government Track, Financial Institution Track, and Consumer Track sought sealing pursuant to the protective order solely because Defendants designated the materials “Confidential.” Defendants have articulated why they want the materials kept under seal – (1) danger from potential hacking of their systems, (2) competitive harm, and (3) that it would undermine current investigations. (ECF No. 333). None of these reasons satisfy the high burden Defendants must meet to rebut the presumption of access and maintain these judicial records under seal.

First, Marriott has stopped using the Starwood reservation system that was hacked. *See* Congressional Testimony of Arne Sorenson, President & CEO, Marriott International (March 7, 2019). While Defendants cite to three cases in their motion to seal (ECF No. 333), these cases are all distinguishable because the risk in those cases was to current systems in use. There is no danger here that hackers can continue to gain access to a system because the Starwood system is no longer being used. *Cf. Zabran v. Trans Union Corp.*, 2002 WL 31010822, at *3 (N.D. Ill. Sept. 9, 2002) (denying defendants’ motion to seal and holding that company’s “hypothetical hacker scenario [did] not convince the Court that [the company] ha[d] good cause to protect its alleged trade secret”). Second, speculative competitive harm is an insufficient basis to keep these materials under seal under well-established law (*See Minter*, 258 F.R.D. at 124), especially when the database that was hacked is a now-defunct system not being used by Marriott. Third, the contention that releasing these materials would undermine current investigations is unfounded and not borne out by prior data breach cases. Even in the *Equifax* data breach case, Senator Elizabeth Warren conducted an investigation of how that breach happened and these materials were all released to the public while other investigations were pending.² Thus, Defendants cannot meet their burden to keep these materials from the public.³ Plaintiffs ask that the Court unseal these judicial materials, or allow Plaintiffs to file their motion to unseal, as contemplated by CMO 3.

Regards,



Carol C. Villegas

² *See* https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf

³ Even if the Court agrees with Defendants that some technical IT material must be kept from the public, Defendants should be required to minimize the amount of material under seal to that which will actually harm them. Allowing Defendants to redact **all** information (as is currently the case) would not be supported by the First Amendment or common law presumptions discussed herein.