Marriott Order Good News For Cybersecurity Class Action Bar

By **John Reed Stark**

John Reed Stark

The cybersecurity class action bar might be celebrating the holidays a bit early this year.

The enthusiasm stems from a recent judicial letter from Judge Paul W. Grimm, of the U.S. District Court for the District of Maryland, who oversees class action litigation arising out of last year's data breach of Marriott International Inc.'s Starwood guest reservation database.

In his letter, which is essentially a judicial decree, Judge Grimm ordered Marriott to make public a crucial third-party report that will reveal key details about the data breach.

Known formally as a payment card industry forensic investigative report, or PFI report, the report in question can be one of the most powerful evidentiary documents for data breaches involving credit card information.

With respect to Marriott breach-related pending multidistrict class actions filed by consumers, financial institutions and governments, the Marriott PFI report has previously either been severely redacted or sealed off to the public entirely. But now, per Judge Grimm, the First Amendment mandates the Marriott PFI report's public release (perhaps lightly redacted).

On the surface, Judge Grimm's order might look like part of one of the many inconsequential discovery-related squabbles that typically occur during class actions and other litigation. But Judge Grimm's decision could have significant ramifications for plaintiffs filing securities-related and other class actions following data breaches at retail companies.

This article drills down into Judge Grimm's ruling, beginning with a discussion of Payment Card Industry Data Security Standards, or PCI-DSS, and the Marriott class actions, and then offers some advice for retailers who wish to avoid, or at least mitigate, the potential costs and other problematic issues associated with Judge Grimm's ruling.

Retailers, PCI-DSS Compliance and Data Breaches

PCI-DSS is a set of requirements created to help protect the security of electronic payment card transactions that include personal identifying information of cardholders, and operates as an industry standard for security for organizations utilizing credit card information.

PCI-DSS applies to all organizations that hold, process or pass credit card holder information and imposes requirements upon those entities for security management, policies, procedures, network architecture, software design and other critical measures that help to protect customer credit and debit card account data.

When a cyberattack targets electronically transmitted, collected or stored payment card information, whether the retailer has met PCI-DSS compliance quickly becomes an intense area of inquiry. For instance, the card brands may levy significant fines and penalties on retailers that are not in compliance with PCI-DSS.

The PFI Report

Once a data security incident occurs, in order to determine whether the retailer must incur any of the above penalties or pay for any system modifications required to achieve PCI-DSS compliance, the retailer is contractually obligated to hire a specially certified PCI-approved forensic investigative firm, also known as a PFI, from a small and exclusive list of card brand approved vendors (currently composed of 22 companies).

The PFI team then performs a specified list of investigative tasks including writing a final report about the data security incident — the PFI report — that is issued to both the retailer and the various credit card companies. The PFI report then becomes the basis used by the card brand companies to calculate potential fines that will be levied against the acquiring banks. These fees are then passed along to the victim company in the form of indemnification.

The Marriott Breach, the Resulting Class Actions and the Marriott PFI Report

On Nov. 30, 2018, Marriott announced a data security incident involving unauthorized access to the Starwood guest reservation database containing information relating to as many as 500 million guests. Since then, Marriott claims that attackers who breached its Starwood Hotels unit's guest reservation system stole personal data from up to 383 million guests — including more than five million unencrypted passport numbers.

The class action frenzy since these events has been nothing short of astounding. A total of 176 plaintiffs from all 50 states have filed suit against Marriott relating to the Marriott breach. Meanwhile, consumers, financial institutions and governments in various states have filed dozens more, including a securities class action. Ultimately all of the class actions were consolidated into one multi-district litigation in Maryland where Marriott's has its headquarters.

In the Marriot MDL, there are five case tracks — government, financial institution, consumer, securities and derivative. In accordance with the the Private Securities Litigation Reform Act of 1995, Judge Grimm ordered that all discovery for both the securities and derivative tracks be stayed until the resolution of Marriott's pending motion to dismiss. Judge Grimm also provisionally granted a motion to seal Marriott's motion to dismiss the government track action, which included a copy of the Marriott PFI report as an exhibit.

Class Action Motions Concerning the Marriott PFI Report

The lead securities class action plaintiffs sought production of the Marriott PFI report before the deadline for amending its complaint, stating:
Requiring production of the PFI Report and other investigative reports related to the Data Breach prior to the deadline for amending complaints will promote efficiency by ensuring that the allegations conform to the available facts, thus eliminating unnecessary discovery and motion practice over allegations based on "information and belief" that may be inconsistent with facts already developed in the PFI and other investigations ... [and] will greatly facilitate all parties' ability to frame the issues in the case for the Court.

The lead securities class action plaintiffs also argued that the First Amendment mandated the unsealing of the Marriott PFI report, stating:
It is settled law that the First Amendment and common law protect the public's access to judicial records ... 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 ... 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 ... None of these reasons satisfy the high burden Defendants must meet to rebut the presumption of access and maintain these judicial records under seal.

Marriott argued against the unsealing of the PFI report, stating:
Plaintiffs' motion is an attempted end-run around the PSLRA's discovery stay. The PSLRA, which governs the Securities and Derivative Tracks, imposes an automatic stay on all discovery pending resolution of motions to dismiss. Plaintiffs now seek to expose confidential discovery materials in public court filings, so that they can access discovery that federal law bars them from obtaining at this juncture. [In addition], 1) Sealing the information protects it from criminals that could use it to perpetrate "future cyberattacks." Disclosure of the sealed information could, for instance, help hackers hone their strategies ... 2) The compelling governmental interest in shielding ongoing investigations requires keeping certain information sealed; ... and 3) Marriott's concern about offering "competitors insight into certain aspects of Marriott's internal business practices.

Judge Grimm's Decision

In an Aug. 30 letter order, Judge Grimm sided with the plaintiffs and ordered the unsealing of the Marriott PFI report, while assigning a magistrate judge to determine if it should contain any narrowly tailored redactions.

With respect to Marriott's PSLRA arguments, because the unsealing of the Marriott PFI report was of no monetary cost to the Marriott defendants, Judge Grimm noted that the spirit of PSLRA remained intact and respected. Moreover, because Marriott had attached the Marriott PFI report to their earlier pleading, Marriott had rendered the Marriott PFI report a pleading and not discovery material which did not run "afoul with the PSLRA discovery stay."

With respect to Marriott's other arguments, Judge Grimm wrote:
Defendants argue (without explaining how) that the information could help hackers attack systems Defendants currently use by studying "network infrastructure for handling cardholder data, systems and strategies for securing such information and thwarting attacks, encryption and decryption processes and protocols, and activity logging." ... This justification for continuing to seal the entirety of the report is both speculative and generalized. Under this reasoning, none the details of how the Starwood database was compromised could ever be revealed, which would prevent the public from understanding how the data breach occurred in the first place, and it would prevent other entities from learning how to better protect their networks from similar attack. This is hardly in the public interest ... Second, Defendants' assertion that unsealing the pleadings and PFI report would interfere with ongoing investigations is equally conclusory and speculative. While Defendants do claim that ongoing investigations would be jeopardized, it is unclear which investigations would be compromised, or how, and therefore this argument fails ... Lastly, Defendants offer no particularized support for the proposition that sealing the entire PFI report and portions of the Pleadings is necessary to prevent disclosure of commercially sensitive data and internal business practices.

Looking Ahead

For a class action plaintiff, the PFI report is the brass ring of documentary evidence, containing detailed, well-documented and potentially inculpatory opinions and findings relating to the Marriott data breach.

Conducted without any direction, interference or influence from Marriott, and presented without any of Marriott's objections, disagreements, opposition, etc., the Marriott PFI report also provides a timely, unique and wholly unfettered analysis of the data breach. Moreover, obtaining a PFI report early on in a class action can save a plaintiff millions of dollars in discovery-related expenses while also delivering a mammoth strategic advantage.

But herein lies the rub. The PFI report is not necessarily the most reliable or even accurate set of findings:

- The PFI team is engaged and directed by the credit card brands — not the retailer — and can not only be biased but also operates under the cloud of a significant conflict of interest;

- A retailer has little opportunity to object to the findings of the PFI report, and is contractually bound not to participate in the PFI's investigation but rather must stand-down and cooperate fully. In fact, a retailer's diminished role in the PFI report process can become an unexpected and unfair obstacle in determining the true nature and scope of the data breach;

- If the retailer does disagree with any of the findings of the PFI — which is likely given the typical subjectivity and speculation of the malware reverse engineering and digital forensics of any data breach investigation — the retailer has little ability to dispute the facts documented by the PFI prior to unfavorable facts being turned over to third parties, including class action plaintiffs;

- The PFI report typically contains no company addendum or other place to present any of a retailer's objections or other opposition, even when a retailer has spent millions (or even tens of millions) by engaging their own professional forensics firm who has significant objections to the PFI report;

- The intended purpose of a PFI investigation is not necessarily to mitigate damages or help a retailer with an incident response, but rather the PFI's goal is to minimize potential fraud losses to exposed cards and determine compliance with industry rules related to data security. In other words, the PFI team is on the hunt for negligence, carelessness, recklessness, fraud and blame — not incident remediation and future data breach defense; and

- The PFI team will not only be conducting an investigation to determine the risk of payment card exposure from a cyberattack, but also assessing the company's

compliance with the PCI-DSS, which can open up an additional can of worms, perhaps more damaging to a retailer than the data breach itself.

Retailers who experience data security incidents must already deal with a class action blitzkrieg, and Judge Grimm's recent love letter to the class action bar only adds fuel to that firestorm. Retailers should take heed and prepare for its consequences.

One preemptive option for retailers is to conduct table-top exercises of data security incidents at their company, and engage a mock PFI team, comprised of former PFI investigators, to create a mock PFI report.

Reviewing a mock PFI report could then provide a retailer with a better understanding of what to expect from a PFI team and enable the retailer to develop the kind of corporate governance and technological infrastructure that would typically result in a more favorable PFI report.

The mock PFI investigation would also provide unique training for IT personnel and others who will have to work with PFI teams, preparing a company's employees for what is typically an extremely awkward experience, replete with hazards and pitfalls.

Think of it this way: When opening a new restaurant what better way to obtain an "A" health department rating than to hire a former health department inspector to conduct a mock inspection. The same goes for PCI-DSS compliance.

Retailers should also spend more time on the due diligence of selecting a PFI from the 22 digital forensic companies currently on the PCI SSC list. Retailers should study carefully the credentials and track record of PFI team members, ensuring that their selected PFI team is experienced, fair, objective, meticulous and open to discussions and disagreement.

Not to be too cynical but it would also probably help if the law firm managing a retailer's data breach response has prior experience with the PFI team and that the PFI team is concerned about their reputation with the law firm — i.e. that the PFI team relies on the law firm for other business. When there exist competing, outside economic interests at issue, it is only human nature for the PFI team to put their best and most fair foot forward during the course of their engagement.

Given that trying to avert a cyberattack is like trying to prevent a kindergartener from catching a cold during the school year, retailers should take steps now to help facilitate an exculpatory PFI report. Otherwise, a class action liability skirmish may be over before the retailer has even had a chance to enter the battlefield.

John Reed Stark is president of John Reed Stark Consulting LLC. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as chief of its Office of Internet Enforcement.