UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: ALL CASES	MDL No. 1:23-md-03083-ADB-PGL

MDL Order No. 34
(Regarding PBI & Welltok Bellwether Plaintiffs' Motion To Compel Discovery from VCE/VCEC Bellwether Defendants)

LEVENSON, U.S.M.J.

Before the Court is Plaintiffs' Motion to Compel various Vendor Contracting Entity Defendants ("VCEs") to provide information regarding the VCEs' own cybersecurity practices, [ECF No. 1774 ("Pls.' Mot. to Compel")]. [ECF No. 1775 ("Pls.' Mem.") at 13–21]. The VCEs are businesses that did not themselves contract with Progress or directly use Progress's MOVEit file transfer program.[1] See [id. at 4]. Plaintiffs also seek to compel production of information regarding whether (and how) various VCEs derived value from the Plaintiffs' data that was "shared with their Vendors." [Id. at 5, 21].

[1] The parties acknowledge that one entity, MLIC, sits a degree further removed from the MOVEit software, making it a VCEC. See [Pls.' Mem. at 4 n.1]. That doesn't matter to this decision.

I. VCES' OWN CYBERSECURITY PRACTICES

A. The Parties' Positions

Plaintiffs contend that the VCEs have interposed overly broad objections in refusing to provide virtually any information about the cybersecurity measures that the VCEs employed for their own systems. [Pls.' Mem. at 13–21]. The VCEs, for their part, insist that their broad objections are warranted. The VCEs contend that information about their internal cybersecurity practices is irrelevant because they did not themselves use the MOVEit product and did not themselves control the servers that were breached. [ECF No. 1787 ("Defs.' Opp.") at 10–21].

B. Legal Standards

The legal standards that govern the scope of discovery are easily recited. Federal Rule of Civil Procedure 26(b) permits "discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." Fed. R. Civ. P. 26(b)(1). In weighing proportionality the Court must consider, among other factors, "the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." Id. "Information within this scope of discovery need not be admissible in evidence to be discoverable." Id.

The challenge, of course, is in applying these general principles in a particular case. Invariably, the importance of information and the balance of benefit and burden tend to look very different to a requesting party and a producing party.

C. Relevance of VCEs' Own Cybersecurity Measures

The VCEs' core assertion is that their own cybersecurity measures are irrelevant because it's not their systems that were breached. [Defs.' Opp. at 10–15]. Plaintiffs attempt to parry this

thrust by pointing to various ways in which the Court has already opened the door to discovery that arguably touches upon internal security. [Pls.' Mem. at 4, 6–7, 11–12, 14]. On the merits, Plaintiffs argue that VCEs' own cybersecurity practices may shed light on the reasonableness of their conduct with respect to the selection and oversight of the vendors whose servers were breached. [Id. at 14–17].

1. Plaintiffs' Claims

Much of the parties' debate turns on their respective (selective) readings of the Court's decision on the motion to dismiss, [ECF No. 1517 ("Order No. 23")]. With respect to the VCEs, Defendants read the order as limiting Plaintiffs to a single theory of liability: the alleged failure to properly vet vendors. [Defs.' Opp. at 5–6, 11–13]. Plaintiffs respond that merely because the Court identified the inadequate vetting theory as a potentially viable legal claim, that does not necessarily mean it is the only claim that Plaintiffs may pursue. [ECF No. 1806 ("Pls.' Reply") at 3–4].

On the theoretical point, Plaintiffs come out ahead. There is language in the Court's decision that leaves the door ajar for other possible legal theories. See [Order No. 23 at 21 ("Even though Defendants did not know about this particular vulnerability prior to the attack, if they failed to take proper precautionary measures or failed to adequately vet their vendors, that is sufficient for proximate causation." (emphasis added))]. In this discovery dispute, however, the questions before the Court are more practical than theoretical.

When it comes to assessing proportionality under Rule 26(b), the questions come down to: What are we looking for? Why does it matter to this case? And—if it is material—how burdensome is it to look for it? To get at these questions, reading between the lines of the Court's decision on the motion to dismiss isn't very helpful. It is more instructive to focus on the complaint itself, [ECF No. 1543 ("Complaint")], and, in particular, on the factual allegations

that concern the PBI and Welltok VCEs. That brings us to, inter alia, paragraphs 2010–2024 (for the PBI VCEs) and paragraphs 3390–3397 and 3464–3465 (for the Welltok VCEs). [Id.].

Looking at the allegations of the Complaint, it is evident that Plaintiffs have not literally restricted themselves to an inadequate "vetting" theory, although a pertinent section is captioned, "Vetting Vendors." [Complaint ¶¶ 2021–2024, at 555–56]. With respect to the PBI VCEs, the Complaint also mentions "routine audits" along with proper vetting. [Id. ¶ 2022]. With respect to the Welltok VCEs, the Complaint mentions failure to properly implement FTC guidelines on data security, [id. ¶¶ 3390–3397], and "fail[ure] to provide adequate oversight of Welltok's data security practices," [id. ¶ 3465]. That said, the factual allegations of the Complaint with respect to the VCEs are overall oriented toward steps that VCEs could or should have taken to assure themselves of the adequacy of the vendors' cybersecurity practices, and—importantly—the only plausible allegations of harm causation turn on the VCEs' selection, vetting, monitoring, or oversight of their vendors.

So, how does evidence about the VCEs' own cybersecurity practices fit with the factual allegations of the Complaint? To get at this question, I asked the parties "to address the question of how to differentiate between truly 'local' cybersecurity measures (e.g. configuration of a firewall on a particular server) and cybersecurity practices that may be implemented locally but that bear on more general risks (e.g. practices regarding encryption of sensitive information)." [ECF No. 1770 (e-order dated April 10, 2026)]. My inquiry assumed (1) that some limiting principle was required, to avoid an endless, open-ended inquiry into VCEs' "local" cybersecurity practices and instead to focus on information that would be relevant to causation and fault with respect to the MOVEit breach; and (2) that it was at least possible that "local" practices could be

relevant. What I was looking for—and continue to look for—is primarily a fact-based argument that would link the information Plaintiffs request to the legal claims they advance.

Plaintiffs' fact-based arguments are not very compelling.

The gist of Plaintiffs' main argument is that if VCEs were sloppy in their own cyber hygiene practices, such general slovenliness might have carried over to their selection and supervision of vendors. See, e.g., [Pls.' Mem. at 15–16 ("As with the TIAA example, if the VCEs are not using WAFs, they likely did not ensure Welltok or PBI did, and it bodes poorly for the continued safety of the Plaintiffs' data which the VCEs still possess.")]. One problem with this argument is that it suggests no workable limitation on the scope of discovery—any deficiency could be indicative of unsound attitudes or practices. Another problem is that whether the VCEs' own practices "bode[] poorly" is not really the question here: What did the VCEs do, or fail to do, that contributed to or caused the harm from the MOVEit breach?

There is considerable force in Defendants' riposte that the best evidence of whether VCEs employed sound vetting practices is VCEs' vetting practices. See [Defs.' Opp. at 12 ("[T]o the extent Plaintiffs want to know whether the VCEs ensured their Vendors followed specific cybersecurity standards, that information has already been captured by the vetting-related discovery about which there is no dispute.")]. Assuming Defendants' term "vetting-related" is understood to encompass ongoing efforts such as auditing, monitoring, and the like, the point is sound.

Plaintiffs point to the allegations, [Complaint ¶¶ 3390–3397], that recount, in generalized terms, the Welltok Bellwether Defendants' failure to follow FTC guidelines. [Pls.' Mem. at 16]. Here too, what's missing is connective tissue linking such alleged failures to the MOVEit breach.

Absent some plausibly alleged chain of causation, Plaintiffs fail to explain the relevance of these general allegations about the Welltok VCEs' own cyber hygiene to the claims in this case.

As a secondary argument, Plaintiffs suggest that the Court has already opened the door by including some such materials in the Defendants' Fact Sheets. [Pls.' Mem. at 7]. They quote, in particular, my comment—in connection with Fact Sheets—that "these kind of things" may be "useful in assessing what was known and what was knowable to the parties at the time." [Id. (quoting ECF No. 1324 at 51)]. But sifting through the Court's words when talking about a different issue is no more persuasive than attempting to distill a ruling about the scope of discovery from the wording of the Court's order on the motion to dismiss. To state the obvious, just because a broad survey of known and knowable risks made sense at a preliminary stage of discovery does not mean that a more detailed inquiry makes sense now. If the preliminary disclosures had surfaced useful, or even promising, materials, those would undoubtedly be the centerpiece of Plaintiffs' follow-up demands. Instead, Plaintiffs merely suggest that they should be allowed to keep going because they got past the first gate.

Plaintiffs also bolster their argument by recounting some of the stop-start discussions between the parties that have led to the present impasse. [Pls.' Mem. at 8–12]. Defendants have their own take—which includes an argument that it's too late in the day for Plaintiffs to press their claims. See [Defs.' Opp. at 18–19]. Such disputes are ubiquitous in multiparty litigation, but—short of gross misconduct—little is gained by trying to sort out who has the better of the quarrel (I assume both sides are sincere in their conviction that the fault lies with the other). The question for the Court remains the same: What kind of discovery is appropriate in light of the proportionality standards of Rule 26?

Both sides point to decisions by other courts that address similar issues, and offer their sharply divergent views about the significance of those decisions: Cheng v. Cal. Pub. Emp.'s Ret. Sys., No. 23-cv-10718 (Cal. Super. Ct.), see, e.g., [Pls.' Mem. at 17–18 (citing ECF No. 1733-7)]; Crowe v. Managed Healthcare of N. Am., Inc., No. 23-cv-61605 (S.D. Fla.), see, e.g., [Pls.' Mem. at 20 (citing ECF No. 1733-8)]; In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig., No. 19-md-02904 (D.N.J.), see, e.g., [Pls.' Mem. at 18–20 (citing, inter alia, ECF No. 1733-9)]. I find these cases to be broadly helpful in illustrating the ways different judges have grappled with similar issues. But none of them offer a straightforward answer to the precise question before me.

All of this leads me back to where I started, facing a fact-bound inquiry about the potential relevance of information regarding the VCEs' own cybersecurity practices. At bottom, Plaintiffs' theory of relevance is too attenuated to warrant the range of discovery they seek. Even if the claims at issue are a bit broader than the "vetting-only" characterization that Defendants urge, discovery must nevertheless be aimed at fleshing out existing allegations—it is not an invitation to commence a generalized dredging operation, in hopes that some unknown nuggets of information might turn up. The Federal Circuit observed, some time ago, that "[t]he discovery rules are designed to assist a party to prove a claim it reasonably believes to be viable without discovery, not to find out if it has any basis for a claim," Micro Motion, Inc. v. Kane Steel Co., 894 F.2d 1318, 1327 (Fed. Cir. 1990) (emphasis in original) (citations omitted). Although the rules have changed somewhat, this principle still applies.

2. Burden of Production

Plaintiffs have a point when they complain that Defendants fail to provide meaningful support for their assertion that the discovery at issue here would be unduly burdensome. See [Pls.' Mem. at 20–21]. Particularly unhelpful to the Court is Defendants' elaborate effort to

explain how a maximalist reading of Plaintiffs' discovery requests could be exceptionally broad. See [Defs.' Opp. at 16–19]. The challenge for the Court is not to figure out whether a particular request for discovery can be read in a way that would yield absurd results. The challenge is to identify a fair and reasonable (i.e., proportional) approach to discovery. I am also skeptical of Defendants' contention that it's too late in the day for Plaintiffs to press their demands. See [id. at 18–19]. Not only does this kind of argument tend to reward parties that drag their feet in resisting disclosures, it also incentivizes parties seeking discovery to rush into court with disputes that are best addressed by consultation and compromise.

In any event, the adequacy of Defendants' showing of burden or timeliness isn't really at issue. The question of burden only comes into play after the demanding party has made a threshold showing of relevance. See, e.g., Controlled Kinematics, Inc. v. Novanta Corp., No. 17-cv-11029, 2019 WL 3082354, at *2 (D. Mass. July 15, 2019) (citing Aronstein v. Mass. Mut. Life Ins. Co., No. 15-cv-12864, 2017 WL 2818993, at *2 (D. Mass. June 29, 2017)). Here, for the reasons discussed above, Plaintiffs fail to surmount that first hurdle.

3. Particular Requests

I have considered Plaintiffs' particular demands individually. None of these has the kind of special relevance that could overcome the broad point discussed above. The core problem is that the VCEs' own cybersecurity practices are insufficiently relevant to the claims in this case to warrant further discovery.

i. RFP B

RFP B requests a diagram of the VCEs' networks. [Pls.' Mem. at 15]. Plaintiffs contend that some information gleaned from such diagrams could be pertinent to their claims. They cite, by way of example, that the use of a WAF (or not) might be indicative of the VCEs' attention to whether their vendors employed a WAF. [Id. at 15–16]. As discussed above, this is a very

indirect way of getting at information that can be probed directly. At best, any evidence gleaned might arguably reflect some generalized tendency to overlook some kinds of security issues. Such inferences about tendencies are too thin to warrant further discovery on the point.

ii. RFP C

Plaintiffs' request for documents pertaining to the VCEs' practices with respect to the retention of PII and PHI on their own systems, see [Pls.' Mem. at 16], is tangential to the question of whether the VCEs took adequate precautions in selecting and overseeing the vendors whose systems were breached. Here too, there is not a strong enough connection between the information sought and the well-pleaded claims in the case to warrant more discovery.

iii. RFP D, RFP E, and Rog A

Plaintiffs request information about the cybersecurity tools and standards employed by the VCEs. See [Pls.' Mem. at 16–17]. Plaintiffs assert that "VCEs have a duty to protect class members' personal data, and Plaintiffs must prove that the VCEs were negligent in their duty." [Id. at 16]. What this formulation elides is that this case is not about "negligence in the air," Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 102 (1928) (citations omitted); it's about alleged breaches of duty that could plausibly have caused or contributed to the vulnerabilities that were exploited in the MOVEit breach. To be relevant, any negligence must also be causally linked to the harm at issue in this case. Here, the only apparent line of inference is that if the VCEs were sloppy in their own housekeeping, they may have been sloppy in scrutinizing the housekeeping of their vendors. That is far afield from the question whether the VCEs properly vetted and supervised their vendors.

Plaintiffs note that some VCEs have already responded to these requests and urge that the other VCEs should do so as well. See [Pls.' Mem. at 17]. But Plaintiffs point to nothing in the materials they have already received that would support ordering more VCEs to respond.

iv. Rog B

Rog B concerns prior breaches that VCEs may have suffered. [Pls.' Mem. at 17]. Here the argument for relevance is only slightly stronger. The idea seems to be that prior breaches should have been a wake-up call for the VCEs and might have alerted VCEs to particular risks that would appropriately have been topics for their vendor vetting process. Again, the causal connection is too attenuated. The applicable standard of care in this case will focus on the precautions that a VCE would be required to take in the exercise of reasonable care with respect to selection and oversight of vendors handling sensitive data. That standard of care is the same whether the VCE has itself suffered a data breach or has relied on a cybersecurity consultant to identify pertinent risks.

As outlined in the Complaint, the case against the VCEs hinges on the reasonableness of their efforts in selecting and overseeing their vendors. The VCEs' own "local" cybersecurity practices and experiences are tangential to that issue.

II. VALUATION OF COMPROMISED DATA

A. The Parties' Positions

In RFP N, Plaintiffs seek discovery regarding the economic value, to VCEs, of data that may have been stolen or compromised in the MOVEit breach. [Pls.' Mem. at 21]. While one VCE has apparently responded to the request, others have objected. [Id.]. Plaintiffs contend that such information is at least potentially relevant to the consideration of damages. [Id.]. Defendants contest the relevance of such data since, in the circumstances of this case, there is nothing to suggest that any harms to Plaintiffs will correspond to the economic value that the VCEs may have derived from the data that was ultimately compromised. [Defs.' Opp. at 22–23].

The legal theories at issue are challenging.

In support of their request, Plaintiffs point to two cases that touch upon the question of assessing damages in a data breach case by considering some measure of the economic value of the information at issue: Smallman v. MGM Resorts Int'l, 638 F. Supp. 3d 1175 (D. Nev. 2022); and In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 341 F.R.D. 128 (D. Md. 2022), class cert. vacated, 78 F.4th 677 (4th Cir. 2023). Both cases highlight difficulties in figuring out an appropriate measure for the harm that individuals suffer when their personal data is compromised. See Smallman, 638 F. Supp. 3d at 1190–91; In re Marriott Int'l, 341 F.R.D. at 153–54. Both cases ponder the possibility that the existence of an illicit dark-web market for stolen data might suggest a measuring stick for gauging losses. See Smallman, 638 F. Supp. 3d at 1191; In re Marriott Int'l, 341 F.R.D. at 154. But that's a very different proposition from measuring the economic value of data to VCEs who use it for legitimate purposes.

Neither case spells out precisely what a successful showing of loss might look like—let alone explain the relevance of a legitimate user's valuation to such a showing. Smallman addresses a motion to dismiss and is therefore concerned with the plausibility of a loss theory, as pleaded. There is language in the decision that suggests the court may have viewed as colorable the idea that a loss computation could somehow be linked to the market for stolen data. See 638 F. Supp. 3d at 1191. On the other hand, Smallman quotes, and seems to rely on, a decision in In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447 (D. Md. 2020), which notes—commonsensically—that "the value of consumer [PII] is not derived solely (or even realistically) by its worth in some imagined market place where the consumer actually seeks to sell it to the highest bidder, but rather in the economic benefit the consumer derives from being able to purchase goods and services remotely and without the need to pay in cash or a check," id. at 462. Smallman, 638 F. Supp. 3d at 1191. A subsequent decision in the Marriott

case—the one that Plaintiffs cite—doesn't advance the ball much further. At the class certification stage, the court in Marriott concluded that there wasn't enough in the record to support Plaintiffs' proposal to measure market value using the breached entity's "own valuation of the monetary value of . . . PII to" that entity. 341 F.R.D. at 154 (emphasis in original). Indeed, the court described that methodology as "disconnected from . . . the conceptualization of Plaintiffs' [loss of market value] theory"—but left the door open for its further development. Id.

In short, Defendants correctly point out that neither of Plaintiffs' cases accepts or adopts their proposed approach for determining damages. [Defs.' Opp. at 22].[2]

Where does this leave us? It appears from the cases that no one has yet successfully threaded the needle in connecting market valuations of stolen PII to loss computations in a data breach case. There are thorny legal issues here. If, ultimately, those issues need to be sorted out, it will make sense to do so with a developed factual record. It seems foolish to try to resolve the issues a priori on the record as it now stands. At the discovery phase, it makes more sense to find out whether any responsive documents exist, and to leave for a later stage of litigation the sorting of inferences and legal conclusions that the parties might draw from such documents.

This entire dispute may be moot, in any event. Defendants assert that "Sutter Health, Virginia Mason, CHI, and OSF are presently unaware of any documents responsive to RFP N, and would have informed plaintiffs as much (or followed up on specific asks) had plaintiffs

[2] Defendants further point out that, in yet another decision in the Marriott data breach litigation, In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 602 F. Supp. 3d 767 (D. Md. 2022), the court rejected a different methodology for determining market/inherent value damages. [Defs.' Opp. at 22–23]. In a detailed analysis, the Marriott court found that the proffered approach could not withstand the pressure testing required for admission of expert opinion testimony under Federal Rule of Evidence 702. See 602 F. Supp. 3d at 783, 789–91. The court did not necessarily reject the notion that—with proper expert opinion support—some kind of market or inherent value theory might be viable.

properly met and conferred on this topic." [Defs.' Opp. at 22]. Rather than decide whether data that may not exist would theoretically be relevant, depending on the validity of one or more legal theories that have not yet been articulated, I will order Defendants to respond to RFP N by confirming whether or not they have any responsive documents. To this extent only, Plaintiffs' Motion to Compel is **ALLOWED**.

III. CONCLUSION

For the foregoing reasons, Plaintiffs' Motion to Compel is **DENIED** with respect to information about VCEs' own cybersecurity measures, and **ALLOWED** with respect to requiring Defendants to respond, to the extent described supra, to RFP N.[3]

SO ORDERED.

May 8, 2026

/s/ Paul G. Levenson
PAUL G. LEVENSON
U.S. MAGISTRATE JUDGE

[3] The parties are advised that under Rule 72(a) of the Federal Rules of Civil Procedure and Rule 2(b) of the Rules for United States Magistrate Judges in the United States District Court for the District of Massachusetts, any party seeking review by a district judge of these determination(s) and order(s) must serve and file any objections within fourteen days of being served a copy of this Order, unless a different time is prescribed by the magistrate judge or the district judge. See Fed. R. Civ. P. 72(a). Such objections must specifically designate the order, or part, to be modified or set aside and the basis for objection. The district judge will set aside any portion of the magistrate judge's order that is found to be clearly erroneous or contrary to law. The parties are further advised that failing to follow the objection procedures of Rule 2(b) may preclude further appellate review. See Phinney v. Wentworth Douglas Hosp., 199 F.3d 1, 4 (1st Cir. 1999); Sunview Condo. Ass'n v. Flexel Int'l, Ltd., 116 F.3d 962, 964–65 (1st Cir. 1997).