1. A decision from the U.S. District Court for the Southern District of New York ordering the plaintiff to implement added data security measures to certain electronically stored information produced by the defendant and declining to shift the costs of such added data security measures to the defendant.

In *United States v. Anthem, Inc.*, No. 20-CV-2593 (ALC) (KHP), 2024 WL 2982908 (S.D.N.Y. June 12, 2024), U.S. Magistrate Judge Katharine H. Parker addressed the issue of data security in discovery and how costs for such security should be allocated between the parties.

In this action under the False Claims Act, the government alleged that Anthem knowingly disregarded its duty to ensure the accuracy of risk adjustment diagnosis data that it submitted to the U.S. Department of Health and Human Services. *Id.* at *1.

During discovery, Anthem anticipated producing to the government the medical information and records of Anthem's members, but the parties disagreed regarding the safeguards and security that the government would apply to this data once in its possession.

The government proposed a "robust set of protections" for the data that included a "bespoke platform, not connected to the internet, accessible by only ten individuals." The data on the platform would be "encrypted at the file level" and would be transferrable only by encrypted physical storage. The government reported that the monthly cost for this level of security was about $5,000/month.

Anthem disagreed that the government's security procedures were sufficient and requested additional protections that Anthem claimed were "consistent with industry standards and with applicable regulatory guidance." These included tracking and logging of all activity on the platform (not just of data moving in or out of the system); monitoring of internal activity logs; certain data loss prevention controls to mitigate potential security gaps in transfer protocols; and certain measures to address security vulnerabilities in the event of a future data breach. These additional measures would cost an additional $4,300/month.

Magistrate Judge Parker began her analysis of the parties' dispute by explaining that "there is a presumption that the responding party bears the expense of complying with and responding to discovery requests and of preserving its own information for litigation," but "the cost of maintaining the security of data turned over in litigation is a slightly different question." *Id.* at *2. She noted that parties generally do not address "secure storage of data or who bears the costs of protecting electronically stored information produced in discovery." However, she pointed out that her model protective order contains a provision that "[t]he producing party may specify the

minimal level of protection expected in the storage and transfer of its information" and the parties' protective order in the case incorporated this model provision.

Magistrate Judge Parker agreed that Anthem's security concerns were valid, pointing to an American Bar Association report that 27% of law firms reported having experienced a security breach and the fact that one of the government's vendors in this case had already experienced a ransomware attack that compromised some of Anthem's data.

Turning to the rules applicable to the parties' dispute, Magistrate Judge Parker began with 26(c)(1)(B) granting courts discretion to allocate expenses for disclosure or discovery upon a showing of "good cause." *Id.* at *3. Referring to a prior decision, *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 323 (S.D.N.Y. 2003), she explained that the factors relevant to analyzing which party should bear the cost of electronic discovery include 1) "the extent to which the request is specifically tailored to discover the relevant information"; 2) "the availability of such information from other sources"; 3) "the total cost of production, compared to the amount in controversy"; 4) "the total cost of production, compared to the resources available to each party"; 5) "the relative ability of each party to control costs and its incentive to do so"; 6) "the importance of the issues at stake in the litigation"; and 7) "the relative benefits to the parties of obtaining information." But Magistrate Judge Parker noted that these factors were developed "over twenty years ago in the infancy of electronic discovery" and were "informative" but "not all directly relevant to the question of whether a producing party who wishes a certain level of data security be provided for data produced in discovery can require the receiving party to bear the full cost of such data security protections for the duration of the litigation until the data is destroyed or returned."

Magistrate Judge Parker identified a list of "non-exclusive factors as relevant to determining whether there is good cause to shift all or a portion of costs of data security measures from the receiving party to the producing party," which included 1) "the nature of the information to be protected and risks and costs associated with unauthorized disclosure of such information"; 2) "the reasonableness of the security measures requested by the producing party (which can include an evaluation of the degree of risk mitigated by the security requested relative to less costly security measures)"; 3) "the cost of the data security requested relative to the overall costs of discovery and amount in controversy"; and 4) "relative ability of the parties to pay the costs of the security requested by the producing party".

Addressing each of these factors in turn, Magistrate Judge Parker found that the first factor, the nature of the information to be protected and risks and costs associated with unauthorized disclosure, weighed against shifting the costs of that security to

Anthem. She reasoned that the medical information at issue was often the subject of cyberattacks, and the costs associated with compromise of the information were high. As a result, Anthem's concern for the security of the data was reasonable.

Magistrate Judge Parker found that the second factor, the reasonableness of the security measures requested, also weighed against shifting the costs of data security to Anthem. *Id.* at *4. She explained that while the system proposed by the government was already secure and took into account health industry standards for protection of information, Anthem was the only party to submit a technical opinion regarding the safeguards offered by the parties. She concluded that she could not "rely on the representations of lawyers for the government to conclude that their proposed safeguards are sufficient."

Magistrate Judge Parker found that the third factor, the cost of the data security requested relative to the overall costs of discovery and amount in controversy, also weighed against shifting the costs of data security to Anthem. She reasoned that the annual costs of Anthem's proposed additional security measures ($60,000 per year) were a "rounding error" relative to the entire amount in controversy.

Finally, Magistrate Judge Parker found that the fourth factor, the relative ability of the parties to pay the costs of the security requested, weighed "slightly in favor of shifting the costs of data security to Anthem." While both sides had the ability to pay the cost of the additional security, she noted that the government was funded by tax dollars whereas Anthem "generates billions of dollars in revenues and has significant resources to defend this action." However, Magistrate Judge Parker stated that "the disparity in resources and source of those resources is not so great, especially in light of the total cost of litigation and amount in controversy, as to raise concerns that [Anthem] is seeking to make prosecuting the case against it financially untenable."

After balancing these factors, Magistrate Judge Parker held that the additional security measures requested by Anthem were proportionate to the nature of the information sought to be protected, reasonable in light of the only evidence provided on the level of security required, and proportionate to the total amount in controversy and the overall costs of litigation. She therefore ordered the government to implement the added data security measures and concluded that the government had not shown good cause to shift the burden to Anthem to pay for the added measures.