This decision generously provided by

Social Law Library members can access a
comprehensive database of
keyword searchable
Business Litigation Session decisions,
at
http://www.socialaw.com
Not a member and need access to the BLS databases?
Join Social Law Today!

Docket: **1784-3009 BLS2**
Date: **November 27, 2018**
Parties: **COMMONWEALTH OF MASSACHUSETTS, Plaintiff vs. EQUIFAX, INC., Defendant**
Judge: **Janet L. Sanders, Justice the Superior Court**

MEMORANDUM OF DECISION AND ORDER ON DEFENDANT'S MOTION FOR A PROTECTIVE ORDER

This case concerns a massive breach of databases maintained by Equifax, Inc. (Equifax), resulting in hackers obtaining access to credit card numbers and other personal identifying information belonging to millions of people. The Commonwealth of Massachusetts, through the Attorney General, has sued Equifax on behalf of Massachusetts residents whose personal information was stolen. The Commonwealth alleges that Equifax violated Massachusetts law — specifically, G.L.c. 93H, G.L.c. 93A and 201 C.M.R. §17.00 et seq. -- by not adequately protect that information and then, when the breach occurred, by not promptly informing consumers of the breach. The case is now before the Court on Equifax's Motion for a Protective Order in connection with its production of sensitive materials related to its network and cybersecurity program.

The parties agree that special measures must be taken to safeguard these materials from inadvertent disclosure and have exchanged draft protective orders over the past several months. In its motion, Equifax asks this Court to approve its most recent proposal. See Exhibit A to Affidavit of Joan A. Lukey, Esq. While agreeing to many restrictions, the Commonwealth

-1-

proposes to eliminate certain portions of that proposed order, as set forth in a red-lined version of the document attached to the Affidavit of Sara Cable, Esq. as Exhibit 2. This Court concludes that the order as edited by the Commonwealth is sufficient to meet Equifax's concerns.

Before turning to the specific areas of disagreement, this Court makes a few general observations. Equifax's proposed order is unique in the restrictions that it places on the Commonwealth, both in its ability to access materials which are concededly discoverable and also in its ability to analyze and synthesize them. Some of these restrictions not only intrude on attorney work product privilege; they also place real obstacles in the way of the Commonwealth's attorneys in preparing and prosecuting what will prove to be a complex case. Equifax argues that these restrictions are necessary in order to prevent another data breach from occurring. But the Commonwealth has already agreed to many restrictions, and Equifax has failed to demonstrate why these are not enough to address its concerns. Equifax's argument in support of its proposal also presumes a lack of internal procedures within the Office of the Attorney General, but that office is regularly charged with handling and protecting highly sensitive and personal information. That it will violate its duty to safeguard this information is not something this Court is prepared to assume. Some of the restrictions in Equifax's proposed order appear to run only one way in that Equifax's own attorneys are not bound by them. This Court fails to see why the risk of disclosure is greater if documents are turned over to a law enforcement agency, where a similar risk exists where those same materials will be handled and reviewed before their production by the law firm representing the defendant. In short, Equifax has failed to show, through facts or evidence, good cause for the restrictions to which the Commonwealth objects. See Rule 26(c), Mass.R.Civ.P.,

-2-

© 2019, Social Law Library. All Rights Reserved.

The specific areas of disagreement between the parties -- together with the reasons why this Court concludes that the Commonwealth's proposal is sufficient — can be summarized as follows.

1. Equifax proposes to strictly limit access to and use of what it calls "Confidential Security Materials" by producing them only in a virtual data room that it controls. The Commonwealth could view the materials in that room but would be unable to prepare notes about or summaries of at least some of these materials even within the room. [1] At the same time, the Commonwealth would be prohibited from downloading or removing the materials from the virtual data room, including any "derivations, abstracts, excerpts, or summaries thereof." The Commonwealth has agreed to a virtual data room and has also agreed not to download the materials themselves. It objects, however, to the limitations placed on its ability to summarize the materials and to download these summaries and analyses as necessary. This Court agrees with the Commonwealth that these restrictions would unfairly burden the Commonwealth as well as their experts. Indeed, even to take notes on the materials and keep those notes outside of the virtual data room would seem to be prohibited by Equifax's proposed order.

2. Equifax's proposed order designates two categories of confidential materials — Confidential Secure Documents and Confidential Secure Data -- imposing even more stringent limitations on the latter. Although Equifax argues that relatively few documents will be classified as Confidential Secure Data, this Court agrees with the Commonwealth that the creation of two categories effectively gives Equifax the ability to over-designate discovery

---

[1] Although Equifax says that it would enable certain technology within the data room that would allow the Commonwealth to "annotate confidential secure documents, review metadata, and perform text searches," that is not mentioned in its proposed order. Moreover, this functionality would not be extended to a subcategory of documents that Equifax determines to be extremely sensitive --material which it describes in its order as "Confidential Secure Data."

materials as Confidential Secure Data deserving of greater protection. If there is a special concern about a certain document, this is better dealt with on a case by case basis. Moreover, many of the materials that the Commonwealth will be most interested in could be classified as Confidential Secure Data under Equifax's proposal, with their related restrictions.

3. Under Equifax's version, the Commonwealth would be unable to obtain hard copies of Confidential Secure Data that are kept within the virtual data room without first obtaining Equifax's permission. Equifax would then have substantial discretion to redact them. That would pose logistical difficulties where the Commonwealth wishes to use such documents — for example, at a deposition or in connection with a motion. Requiring the Commonwealth to alert Equifax to which documents it views as important also intrudes on the work product privilege. At the hearing, the Attorney General pointed out that the office already has a procedure whereby documents are kept under lock and key, with access to them not only limited but carefully tracked. If hard copies were converted to electronic copies and on an office computer, those computers are all encrypted. This Court has no reason to believe that these measures are not enough.

4. Equifax's order contemplates that no Confidential Secure Materials or any pleadings describing any part of them can be shown to or even described to anyone within the Attorney General's Office except for the two attorneys who have entered an appearance in this case. Although Equifax expressed a willingness to expand this category (so as to include the Attorney General

© 2019, Social Law Library. All Rights Reserved.

herself, for example) these limitations would still pose a significant burden on those working on the case. They could not use staff to assist them with their work, or consult their superiors, for example. These are advantages that Equifax's lawyers would appear to enjoy

under Equifax's proposa1. [2] This Court has no reason to believe that the Attorney General's security measures are any less stringent than those of a law firm.

5. Equifax refuses to produce the Confidential Secure Data in its native form. Its justification for this is that the Commonwealth has no reason for viewing the data in that form because this case is only about Equifax's failure to notify consumers about the data breach. The Commonwealth's claims cannot be construed so narrowly, however. In any event, the rules require that documents be produced in native form — and for good reason. In such a format, they are searchable and the viewer has access to metadata.

For all the foregoing reasons and for other reasons articulated in the Commonwealth's Response, this Court declines to adopt the order proposed by Equifax and that its motion is therefore DENIED. It instead adopts the modified version of that order as proposed by the Commonwealth.

Janet L. Sanders, Justice the Superior Court

---

[2] At the motion hearing, Equifax's counsel stated that her law firm would be bound by these same restrictions but that is not apparent from Equifax's proposal.

© 2019, Social Law Library. All Rights Reserved.