

WHAT IS THE CASE ABOUT?

The 2017 Equifax data breach is deeply troubling, not only for its massive scale, but also for the failure of Equifax to take basic steps to protect itself and consumers from such a preventable catastrophe. The breach—in which hackers entered Equifax's system through a known vulnerability to access names, Social Security numbers, dates of birth and other information—was caused by Equifax's negligence. Quite simply, the credit rating agency failed to heed warnings from security experts to properly secure its U.S. website. Further, Equifax waited nearly six weeks to report the breach to the public.

ICBA's lawsuit asks the U.S. District Court for the Northern District of Georgia (Equifax is based in Atlanta and all Equifax data breach lawsuits have now been transferred this court) to require the credit bureau to compensate community banks harmed by the breach. The complaint cites the myriad damages caused by the breach, such as the costs of customer credit freezes, protective measures to deter and/or prevent fraud, and cancelling and replacing payment cards. For a longer-term solution, ICBA also asks the court to require Equifax to improve its security infrastructure to prevent future data breaches.

WHAT DO COMMUNITY BANKS NEED TO DO TO BE COMPENSATED FOR DAMAGES?

If the Court, as requested, certifies a class of financial institution plaintiffs, community banks will be included and will be eligible to share in any recovery obtained. For a class to be certified, however, some banks must be willing to serve as class representatives. For this reason, interested banks should consider joining the litigation.

HOW DO YOU ESTIMATE DAMAGES INCURRED BY BANKS?

Intangible damages may be measured by what banks have done administratively in the wake of the breach, responding to Equifax's revelations, such as freezing credit and monitoring accounts, and the costs of steps taken to reduce risk (i.e. implementing multi-factor or alternative methods of customer authentication). There may also be regulatory considerations.

Other monetary losses, such as fraud loss or other costs, can also be measured. Previously, in payment card data breaches, plaintiffs have relied on expert testimony and card brand analysis by looking at baseline fraud and comparing it against incremental fraud. Some element of fraud can causally be connected to the universe of cards. In this case, plaintiffs may rely on the same type of analysis—an industry wide experience and then compare a baseline to the incremental fraud for this particular breach. Regardless of how damages stemming from actual fraud are causally related, there are many damages which easily connect—how you change authentication of customers, respond to regulators, and manage the concerns of customers—all of those costs are directly attributable.

IF OUR BANK JOINS THE CASE, DO WE NEED TO ATTEND HEARINGS OR TRIALS?

Generally, these cases rarely go to trial. However, if it does go to trial, the class representatives would attend the trial.

WHERE WOULD DEPOSITIONS OCCUR, IF ANY?

If a deposition were required of a participating bank, it would likely be done at the bank's location.

DO BANKS PAY OUT OF POCKET FOR THE TRIALS AND HEARINGS?

No, the coalition of attorneys advances all costs related to the case.

WHAT IS THE TIME COMMITMENT FOR MY BANK IF WE JOIN THE SUIT?

If the Court certifies a class of financial institution plaintiffs, community banks will be included and will be eligible to share in any recovery obtained. For a class to be certified, however, some banks must be willing to serve as class representatives. The ICBA has sued, but only for injunctive and declaratory relief. A class for damages must still be established. For this reason, interested banks should consider joining the litigation. The bank's time commitment will relate primarily to the discovery process—the formal gathering and exchange of information by the parties in the litigation. As is true in every lawsuit, the parties need to preserve documents and data. The retained law firms for financial institutions will help your bank with this process. This is not usually too disruptive because of the preservation obligations and requirements to which banks are already subject. Next steps will involve gathering data about the breach, including any data, analytics or reports and certain emails; the law firms will again assist your institution in this process. Depending on the amount of data and documents, this usually takes about 4-8 hours of an IT staff person's time—it can be more, or it could be less.

WHO DO I CONTACT WITH SPECIFIC LEGAL QUESTIONS ABOUT THIS CASE OR IF MY BANK WANTS TO JOIN THE SUIT?

Contact Gary Lynch by email at: gary@garylynchlaw.com.

WHO DO I CONTACT AT ICBA REGARDING THIS CASE?

Contact Jeremy Dalpiaz by email at: jeremy.dalpiaz@icba.org.