Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Hundreds of Equifax Data Breach Lawsuits Have Been Filed—What are their Chances?

November 1, 2017

The recent data security breach of Equifax, one of the three main credit reporting agencies, has already spawned scores of federal lawsuits, as individual consumers, financial institutions, and state and local governments have all filed suit against the company. These cases involve a wide variety of federal and state claims, raising a host of legal issues that may more broadly inform Congress's consideration of cybersecurity law going forward.

The impetus for the bevy of lawsuits against Equifax was a data breach that compromised sensitive consumer information (e.g., names, birthdates, Social Security numbers) for over 145 million Americans. The breach, which occurred in mid-summer and was reported by Equifax in September, stemmed from the exploitation of a vulnerability that the credit reporting agency was made aware of in March 2017. (For more details on the breach itself, see this testimony from CRS cybersecurity analyst Chris Jaikaran).

Since the breach, over 200 lawsuits have been filed against Equifax in federal and state courts around the country. The cases brought against the company allege various common law, state statutory, and federal statutory claims. The suits seek monetary damages as well as injunctive relief (e.g., a court order requiring Equifax to implement stronger cybersecurity measures). The lawsuits, however, face a variety of challenges, including with regard to both the *process* of finding a venue that can hear a given case and the *substance* of the underlying claims.

Procedural issues. On the procedural side, one of the biggest hurdles the Equifax plaintiffs will have to overcome in light of recent Supreme Court precedent relates to the constitutional requirement of "standing." This legal doctrine, which derives from Article III's case or controversy requirement, necessitates that parties seeking judicial relief from a federal court show that (1) they have suffered (or will imminently suffer) a concrete and particularized injury that (2) has been caused by the defendant's actions and (3) can be redressed by the court. The Supreme Court recently specified that the injury alleged in a lawsuit must both affect a plaintiff "in a personal and individual way" and be real rather than abstract. Cognizable harms can include incursions on property interests, contractual rights, and, in certain circumstances, statutorily created rights. (There is some question regarding to what extent Congress can functionally create Article III standing based solely on violation of a statutory right.)

In the Equifax cases, plaintiffs may have trouble meeting the standing requirement for several reasons. First, to the extent their claims are based solely on the increased risk of identity theft that they potentially

face due to having their personal information compromised in the breach, courts may be skeptical as to whether any injury that the plaintiffs may suffer is "certainly impending," the standard announced in a 2013 Supreme Court case. Lower courts have split on the question of whether the risk of identity theft alone is a sufficient injury to confer standing on a plaintiff or whether a person must wait until she has actually had her identity stolen before she can sue. The Eleventh Circuit—which includes Atlanta, where Equifax is located and where the litigation reportedly might be consolidated—has not taken a side on the issue. Second, it may be difficult for a plaintiff to prove the causation prong of the standing inquiry because the burden would be on the party seeking federal jurisdiction to prove that any identity theft (or risk thereof) is the result of the Equifax breach as opposed to some other cause.

Beyond the standing issue, other procedural issues that may be raised in the Equifax litigation include:

- Class action certification—Equifax plaintiffs will have to establish that they meet the requirements under the Federal Rules of Civil Procedure to have their claims aggregated into a single suit, such as that there are questions of law or fact common to all of the plaintiffs; and
- Whether their claims will have to be arbitrated—there has been some debate over whether Equifax could require its consumers to bring their claims before an arbitrator as opposed to a court.

Substantive issues. The Equifax data breach plaintiffs also face substantive challenges in bringing their suits. One particularly tricky issue concerns any claims relying on common law torts, like negligence. To prove negligence, a plaintiff must demonstrate (1) that the defendant owed her a duty of care, (2) that the defendant breached that duty, and (3) that as a proximate cause of that breach the plaintiff (4) was harmed. When courts ask whether a defendant has been negligent, the defendant's conduct must be measured against a general standard of care with which it ought to have complied. For example, even if a company follows all of the best cybersecurity practices and is as vigilant as it can be, it may still be possible for sophisticated hackers to nevertheless access the company's networks in unauthorized ways. In such a case, a court would be unlikely to find such a company negligent despite a breach in its security. On the other hand, a company that openly put unencrypted sensitive customer information on a website that it knew could be subject to a breach would be much more likely to be found negligent. Somewhere between these extremes is the relevant standard of care for purposes of a data breach negligence lawsuit.

However, in the data breach context there is no universally agreed upon standard of care for cybersecurity measures. Courts might look to the National Institute of Science and Technology's 2014 Framework for Improving Critical Infrastructure Cybersecurity, relevant state regulations, or industry-created security standards to determine what kinds of actions Equifax should have been taking to protect the sensitive personal information it stored, but it is unclear whether any of these provisions would amount to a standard of care with which Equifax had the duty to comply.

In addition to the standard of care issue, the other elements of a negligence claim are not slam dunks either. The plaintiffs must show they were harmed, and while money spent by consumers to freeze or monitor their credit is easily quantifiable, other injuries such as emotional distress are harder to prove. Also, showing that the Equifax breach was a "proximate" cause of any injury requires proof that the breach was reasonably foreseeable.

Beyond the negligence claims, litigants have sued Equifax under other theories, including violations of positive state and federal laws. Additional substantive questions related to plaintiffs' lawsuits include:

- Whether Equifax's 6-week delay in announcing the data breach violated state data breach notification statutes, most of which require only that notification occur "without unreasonable delay";

-
- Whether the company violated state unfair and deceptive practices laws, e.g., California Business & Professional Code § 17200 *et seq.*;
- Whether the company had reasonable procedures in place to protect consumer data from unauthorized disclosures as required by the Fair Credit Reporting Act;
- Whether Equifax implemented the safeguards promulgated by the Federal Trade Commission pursuant to the Gramm–Leach–Bliley Act;

What's next? The Equifax breach litigation implicates a number of issues that are potentially relevant to Congress as it considers this fast-changing legal area. Several federal bills have been proposed in the wake of the breach, such as to prohibit credit reporting agencies from charging a consumer to freeze her credit, S. 1816, S. 1810, H.R. 3755, H.R. 3878, or to establish cybersecurity standards for credit bureaus, S. 1982, H.R. 4028. The Equifax breach could also affect the perennial debate about whether a federal data breach notification law is necessary—one bill to establish a 30-day deadline for notification to consumers, H.R. 3806, has been introduced in the House.

In the litigation itself, the question of which court will hear many of the suits may be answered soon. Multiple parties, including Equifax itself, have asked the Judicial Panel on Multidistrict Litigation ("JPML") to consolidate the federal cases in a single district court for coordinated pretrial proceedings; the JPML is scheduled to hold hearings on that issue at the end of November. Finally, the breach has also aroused the interest of several federal agencies: the Department of Justice, the FTC, and the Consumer Financial Protection Bureau have all reportedly begun investigations into Equifax's conduct that could lead to civil or even criminal penalties.

Author Information

Austin D. Smith
Legislative Attorney

Disclaimer