

Independent Bank Class Action Alleges Specific Equifax Security Failures, Actual Harm and the Threat of Future Harm

Article By:

Tara M. Swaminatha

India K. Scarver

In another lawsuit against Equifax, the Independent Community Bankers of America (ICBA), on behalf of thousands of community banks, seeks to hold Equifax accountable for the July 2017 data breach that potentially affected more than 145.5 million consumers. ICBA, along with Bank of Zachary and First State Bank, filed the class action last week in the U.S. District Court for the Northern District of Georgia.

In analogous litigation, two open issues exist:

(1) First, whether alleging the *threat of future harm* – as opposed to alleging *actual harm suffered* – is sufficient to establish Article III standing, and

(2) Whether plaintiffs allege defendants' acts or omissions with sufficient specificity.

Article III Standing for Threat of Future Harm vs. Actual Harm Suffered

In the ICBA complaint, since Plaintiffs do allege actual harm suffered, in addition to the threat of future harm, Article III standing is likely established. Specifically, Plaintiffs allege actual harm suffered from having had the immediate need to mitigate and rectify fraudulent transactions (i.e., monetary harm from reissuing cards, stopping transactions, current monitoring efforts, fielding questions from consumers). Plaintiffs allege a threat of future injury from: (i) having to continue monitoring the “certainly impending risk” of fraudulent use of their customers' stolen identities; (ii) further monetary injury resulting from consumer emotional distress – those emotionally distressed consumers may choose to forego banking services, instead opting to use cash, which ICBA argues will hurt revenue from transaction fees, ATM fees, interest and other monetary charges; and (iii) significant costs that will be incurred to implement additional methods to determine customer authentication and credit worthiness.

In analogous litigation, many plaintiffs only allege the threat of future harm. The Supreme Court may settle a circuit split on whether such theoretical harm is sufficient to establish Article III standing. On December 12, the Federal Trade Commission (FTC) holds an open workshop for public commentary

on the topic.

Alleging Defendants' Acts with Sufficient Specificity

Data breach plaintiffs often allege that the mere fact that a defendant suffered a data breach sufficiently demonstrates that the defendant (must have) behaved badly. Absent allegations that a defendant, for example, failed to fix a known insecurity, some courts reject such vague allegations. These plaintiffs face a particular challenge prior to discovery because acts or omissions that could have caused or enabled a data breach are not often public. In the Equifax case, however, Plaintiffs cite allegations of specific wrongdoing likely gleaned from media reports, including that Equifax actively mishandled its data security as evidenced by (i) not following known industry standards and prior recommendations, and (ii) failing to monitor its security systems. All this, Plaintiffs claim, opened the door for hackers to access the personally identifiable information and Payment Card Data of millions of Americans.

Demands

ICBA demands that Equifax compensate community banks and other financial institutions for “misfeasance” in failing to implement recommended security protocols and failing to detect the presence of hackers for weeks. ICBA also demands Equifax employ “adequate” security protocols consistent with industry standards to protect personally identifiable information and Payment Card Data.

© Copyright 2025 Squire Patton Boggs (US) LLP

National Law Review, Volume VII, Number 339

Source URL: <https://natlawreview.com/article/independent-bank-class-action-alleges-specific-equifax-security-failures-actual-harm>