Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Tips For In-House Counsel Anticipating Cyber Class Actions

By **David McDowell and Nancy Thomas** (November 25, 2020, 1:38 PM EST)

David McDowell

Nancy Thomas

Blame the pandemic on yet one more startling statistic: The number of data breaches has increased over 270% as compared to the same period last year.[1]

Cybercriminals have taken advantage of the disruption and distraction caused by the move to work from home. Ransomware is up 90%, according to one report.[2] These criminals have hit every industry, from hotel chains to tech companies to major law firms. Hospitals are the latest victims.

On Oct. 28, the Federal Bureau of Investigation and other agencies issued a joint alert warning of "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers" by international cybercriminals.[3] Five hospitals have been targeted and these attacks could impact hundreds more.

More data breaches mean more data breach class actions. A company announces a data breach, and, a few hours later, plaintiffs lawyers start filing class actions. Here are five things in-house counsel can do as they add litigation to the dozens of other data breach response work streams.

1. Create a strong foundation.

Depending on the nature and scope of the breach, companies can expect dozens if not hundreds of class actions in the days and weeks after announcing a breach. This flurry of action can seem like chaos of the worst kind — the kind with no end in sight. At this early stage, companies need outside counsel who can scale up and handle dozens or hundreds of lawsuits until the filings slow and steer the lawsuits into a manageable posture.

The filing of lawsuits triggers the company's obligation to preserve. Counsel should draft and distribute a legal hold notice and ensure that all auto-delete and similar procedures are disabled while the lawsuits are pending.

2. Impose order on the chaos.

To manage the litigation, the company will want to consolidate the various lawsuits before one court. The company or some number of plaintiffs counsel will typically file a petition before the U.S. Judicial

Panel on Multidistrict Litigation, or JPML. But the process takes time, as discussed below.

In the meantime, local counsel typically handle the day-to-day management of these lawsuits. Local counsel are familiar with local courts and local court rules. So they are in the best position to deploy early procedural motions, such as seeking an extension of time to respond to a complaint or a stay in the proceedings.

Experienced outside counsel will have relationships with strong local counsel in most of the jurisdictions where cases are typically filed and can quickly vet and engage local counsel in any other jurisdictions, often with an assist from the company's insurer. Local counsel report to outside counsel, who streamline communications and coordination with in-house counsel.

3. Keep insurers updated.

Unless self-insured, most major companies have cyberinsurance that covers data breach litigation. Those policies require that the insured provide prompt notice and keep the insurer informed of case developments.

The company's internal risk management team or in-house counsel should send all lawsuits to the insurer in a timely manner and open a dialogue with timely updates. An open and continuous dialogue regarding the lawsuits and litigation strategy will help the insurer understand why the company proposes a particular approach.

This also will benefit the company if and when it wants to consider settlement by providing opportunities for the insurer to understand the strengths and weaknesses of the company's defenses. Discussions with insurers are privileged, so these discussions are generally protected from disclosure.

4. In the meantime, defend against jockeying by certain plaintiffs counsel.

Many data breach class actions are filed by the usual suspects — a set of plaintiffs counsel that have been part of most of the major data breach cases. These lawyers know that the cases will eventually be consolidated, so they do not push to litigate every case. Instead, they file one or more cases as quickly as they can and count on their experience in prior data breach cases to convince the court to appoint them as sole or one of the lead counsel who control the plaintiffs' side of the litigation.

But some plaintiffs attorneys will go against the grain. They will file ex parte motions regarding document preservation or discovery soon after they file their clients' lawsuits in an attempt to put themselves in a position to seek appointment as lead counsel in the consolidated action because their clients' cases are further along.

Most judges see through this gamesmanship and deny attempts to push particular cases forward. Local counsel, though, will have to be prepared to fight these fires even with the low likelihood of success.

5. Expect to wait for the cases to be consolidated.

The JPML determines whether cases filed in federal court will be consolidated for pretrial purposes in a multidistrict litigation. The JPML only sits every other month. As a result, 60 to 120 days can go by before the JPML rules on a request to consolidate lawsuits filed in the wake of a data breach.

When the JPML grants a petition to consolidate lawsuits into an MDL, it assigns the MDL to a particular federal judge. Typically, the JPML assigns data breach class action MDLs to a judge in the federal judicial district where the company's principal place of business is located.

After the JPML assigns the MDL, the clerks of the districts where the original cases were filed will send the dockets for the lawsuits. Typically, the assigned judge holds an initial case management conference a month or two after the assignment. At this conference, counsel discuss the timing for appointing lead plaintiffs counsel in the MDL — usually 45 to 60 days from the conference — as well as the time frame for the plaintiffs to file a consolidated complaint — usually 30 to 60 days after the court appoints lead plaintiffs counsel.

Thus, it can take eight to 10 months or more between the filing of the initial complaint to the filing of a consolidated complaint in the MDL proceeding, which kicks off the litigation of the plaintiff's claims.

Keep Calm and Litigate On

Keeping these points in mind will help in-house counsel efficiently and effectively manage the initial steps in data breach class action litigation.

David F. McDowell and Nancy R. Thomas are partners at Morrison & Foerster LLP.

[1] Ellen Sheng, Cybercrime ramps up amid coronavirus chaos, costing companies billions, CNBC, July 29, 2020, https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html.

[2] Id.

[3] Alert (AA20-302A), Ransomware Activity Targeting the Healthcare and Public Health Sector, Cybersecurity & Infrastructure Security Agency, https://us-cert.cisa.gov/ncas/alerts/aa20-302a (last visited Nov. 6, 2020).