THE VERGE

If the hack doesn't kill Ashley Madison, these lawsuits could

By Russell Brandom on August 20, 2015 01:29 pm

This week, the adultery-themed dating site Ashley Madison was hit with one of the most damaging and personal breaches we've seen, as digital attackers released names, emails, and private profiles for as many as 32 million users worldwide. The group behind the breach said their goal was to destroy Ashley Madison's parent company, Avid Life Media, and they may well succeed. The company is in for an array of damaging and expensive lawsuits, quite possibly enough to drive it into bankruptcy outright. As Casey Newton said yesterday, this is a new kind of breach with a new kind of damage — and that unique damage is going to lead to some uniquely expensive lawsuits.

The biggest concern is a simple class action suit by the company's users. In most data breach cases, the plaintiff's biggest hurdle is proving that the users suffered a tangible harm, a tricky task for hacks like Target's that saw credit card companies and retailers absorb all the immediate financial damage. But for anyone caught up in the Ashley Madison breach, the harm is obvious. Anyone whose email was caught in the data dump suffered obvious reputation damage, simply by virtue of being included. Courts can argue over the exact nature of the harm — and how much the company should pay for it — but it will be very hard to argue there was no harm at all. With this many users involved, the final settlement could easily reach into the hundreds of millions, a catastrophic sum for a company that only grossed $115 million in pre-tax revenue last year.

"Here, unlike most retail breaches, just the fact that one is exposed as a customer of the site is sensitive, confidential, and potentially damaging information," says Goodwin Procter partner Brenda Sharton, who chairs the firm's privacy and data security practice.

> "JUST THE FACT THAT ONE IS EXPOSED AS A CUSTOMER... IS SENSITIVE."
>
> **—Brenda Sharton, Goodwin Procter**

The company's "full delete" feature opens it up to even more litigation. Tens of thousands of users paid Ashley Madison to scrub their names from the database — but because credit card information wasn't fully scrubbed, those users have still been implicated in this week's data dump. As a result, users can sue the company for false claims, and the FTC might even prosecute the company for deceptive trade practices. "Depending upon how that product was advertised and what the consumers were notified about in the site's terms of use and privacy policies, these statements may themselves give rise to fraud and misrepresentation claims if not true," Sharton says. "Regardless of the outcomes, and even if there are strong defenses for the company, the legal fees alone may be staggering."

But ALM's problems are larger than just US courts and regulators. "The other complication is that the website's clients reside in different countries," says Craig Newman, a partner at Patterson Belknap Webb & Tyler. "So you have the laws of different countries that might come into play, some of which value personal privacy greater than others." The bulk of ALM's users were in the US, so the final damages in foreign cases are likely to be smaller, but the cost of litigating the same case across a dozen different legal systems is likely to be significant.

Still, it's too early to write off ALM entirely. The class action suits may not come together, or the company may prove exceptionally well protected against the mounting claims. Cybersecurity law is still a relatively new field, and it's hard to predict how far any given case will go. Sharton also points out that ALM will have a strong civil case against Impact Team if the group is ever publicly discovered — although for now, that seems like an outside chance. "Lots of companies have rebounded from seemingly disastrous hacking events," she says. "I'm mindful that we haven't heard much of ALM's side of the story yet — they may come out stronger for it. Stranger things have happened."

"THE LEGAL FEES ALONE MAY BE STAGGERING."

—Brenda Sharton, Goodwin Procter

In the background of all of the legal claims is a more troubling question: where did Ashley Madison go wrong? The company clearly viewed security as a priority, but aside from holding onto too much data, we have yet to pin down any specific security failures that led to the breach. That will be a central question in any cases that go to trial. "At the heart of many data breach cases is the general question of whether the victimized company employed reasonable data protection measures," says Newman. If the hack is the work of a disgruntled contractor, as ALM initially suggested, then damages could be significantly lower.

But those lingering security doubts could also have real consequences outside the courtroom. Ashley Madison occupies a strange niche among dating services, and even if the company is swallowed up by legal claims, another company could pop up offering the same services with stronger security and smarter data policies. The question is whether anyone will trust them, and if any companies will take the risk. If the legal fallout is messy enough, it might scare companies away from offering adultery-oriented services entirely. If it does, a single hack and a few lawsuits will have shut down an entire corner of the web.

SOURCE URL http://www.theverge.com/2015/8/20/9183093/ashley-madison-hack-lawsuit-class-action-sue