What Is 'Informational Injury'? The FTC Wants To Find Out

By **Ben Kochman**

Law360, New York (December 8, 2017, 6:05 PM EST) -- The Federal Trade Commission will consider on Tuesday when a breach of consumers' data becomes an "injury," at a workshop companies and privacy hawks are watching for clues on what kinds of data breach lawsuits the agency will bring going forward.

Speakers at the event at Washington, D.C.'s Constitution Center, including acting FTC head Maureen Ohlhausen, will grapple with defining when a data breach rises to the level of "informational injury" worth suing over.

The agency has pursued data security cases in the past by using its power to police "unfair and deceptive" practices under Section 5 of the FTC Act. But that approach has come under fire as of late, with small medical testing company LabMD and network equipment maker D-Link claiming that the FTC overstepped its authority by pursuing cases in which the breaches were not likely to cause consumers "substantial" harm.

Trade associations for tech companies, retailers and advertisers **sang a similar tune** in dozens of public comments filed in advance of Monday's event, urging regulators to focus on concrete harms that can stem from data theft and misuse — like fraudulent charges placed with stolen credit card data, for example — and to steer away from what some attorneys call "theoretical" injuries, such as the fear of future theft.

"By legitimizing informational injury, we open up a giant Pandora's box of things the courts have not recognized as injuries up to this point," Gerry Stegmaier, a partner in the IP, Tech and Data Group at Reed Smith LLP, told Law360 this week.

"The term 'informational injury' is a way to get past what has been the biggest hurdle for plaintiffs in these lawsuits," said Shook Hardy & Bacon LLP data security and privacy group chair Al Saikali, citing federal courts' dismissals of some data breach suits on grounds that a party has not demonstrated an injury.

Ohlhausen, the FTC acting chairman, offered some hints as to her take on the matter at a speech to a group of communications attorneys in September, in which she gave five examples of what she called "consumer informational injury."

The agency can make a "deception" informational injury claim in cases where a company misleads customers about its privacy practices, she said, citing a 2011 case accusing Google of signing up users of its Gmail service to its social network Google+ without permission.

Speaking to the Federal Communications Bar Association, Ohlhausen also cited direct financial harm to victims of a recent data breach at Wyndham Hotels, where there were reported fraudulent charges and identity theft. Ohlhausen included the hassle of reporting identity theft as an "indirect" cost.

Other potential informational injuries the FTC head cited included health or safety injury, found

in harassment resulting from a revenge porn operator's posting of intimate photos, unwarranted intrusion — a company that secretly installed monitoring software on rental computers, for example — and reputational harm, which Ohlhausen noted the FTC had never cited as reason alone to bring a case.

Ohlhausen said she planned at Monday's workshop to hone in on the "qualitatively different types of injury to consumers and businesses from privacy and data security incidents," as well as figure out how to measure those injuries and estimate their risk.

"Ultimately, the goal is to inform our case selection and enforcement choices going forward," she said in her September speech.

Former FTC official Phyllis Marcus, now a partner at Hunton & Williams LLP, called Monday's event an "interesting intellectual exercise" — but warned that clarity on the FTC's approach is unlikely to emerge until cases are filed.

"People who are looking for more bright-line guidance, I just don't think that that's what's going to happen here," she told Law360. "You're more likely to see it in terms of the kinds of cases that are pursued, or conversely, the kinds of cases that won't be pursued."

Stegmaier, who has defended consumer privacy class actions, said it would be productive to have a frank discussion about the specific fallout consumers face, or don't face, when their information is compromised.

"The reality of compulsive breach notification laws is that there is an enormous amount of noise about security breaches, but virtually no public discussion about the consequence of the information being breached," he said.

--Additional reporting by Allison Grande. Editing by Pamela Wilkinson and Kelly Duncan.