Lenovo Invites Legal Maelstrom With Superfish Adware

By **Cara Salvatore**

Law360, New York (February 25, 2015, 8:35 PM ET) -- With security experts and consumers up in arms over recent revelations about its harmful adware known as Superfish, computer maker Lenovo has found itself facing at least four privacy class actions, a consolidation request and, attorneys say, more legal headaches to come.

The four putative class actions filed in recent days — one in North Carolina federal court and three in California — are likely just the start, experts said, considering Lenovo's decision to covertly install adware that security experts say could allow hackers to steal laptop users' personal information. The move practically invites large-scale legal action, attorneys say.

"Rumor is that there are going to be several more filed," Mark Dearman of Robbins Geller Rudman & Dowd LLP, which is co-counsel in one of the four suits, told Law360 on Wednesday.

Dearman's firm filed a motion Wednesday to consolidate the suits in multidistrict litigation in the Eastern District of North Carolina.

The Superfish software at the heart of the controversy was installed on a range of Lenovo laptops that were first sold in September. The software breaks HTTPS encryption and makes information easily available to anyone nearby sophisticated enough to grab the unencrypted data from Wi-Fi.

"The company actually worked with another party to invent code that would enable [hackers] to access info. It's just wrong. It's flat-out wrong," said Bill Munck, a tech attorney with Munck Wilson Mandala LLP out of Dallas.

"It's kind of like a fox sneaking into a farm," he added. If the fox searches around the entire perimeter of the farm and finally digs a hole under the fence, "that doesn't mean the farmer isn't doing his job. But in this case, the guy who's putting in the fence is actually leaving holes intentionally."

The hole in Lenovo's fence was first noted on a message board on Dec. 7. It was referenced separately on a Lenovo corporate message board on Jan. 21. And the most damning reveal emerged on Feb. 18, when security researchers Chris Palmer and Kenn White posted screenshots on Twitter showing that a supposedly secure certificate from Bank of America was signed and verified via Superfish, not the bank as should have been the case.

In an open letter sent Feb. 23, Lenovo Chief Technology Officer Peter Hortensius said, "For [laptops] already in use, Superfish will be removed when their antivirus programs update."

But the company's pledge will not stop the tide of litigation, experts say. Catherine Meyer, a

senior counsel at Pillsbury Winthrop Shaw Pittman LLP, said the Superfish scandal was exactly the type of situation that drives plaintiffs to the courthouse.

Meyer and others stressed that while Lenovo will likely continue to find itself on the receiving end of a deluge of class actions, the company will have strong defenses because there are few laws that fit this type of alleged consumer harm.

“The problem with privacy and computer litigation is there are very few laws that address this,” Meyer said. “[But] as long as companies are willing to settle and pay for something, people will sue.”

Besides the difficulties in finding a law friendly to their claims, plaintiffs also have to contend with standing issues and proving that they were actually harmed by the vulnerability.

“I’m not sure the consumer right of action would survive, to be honest,” said Hsiao "Mark" Mao, a partner with Kaufman Dolowich & Voluck LLP. “They would have to prove damages … there’s a big debate right now in consumer actions as to what exactly damages are.”

Lawyers in the four suits seem to be aware of the possible difficulties because they've thrown the proverbial kitchen sink at Lenovo and Superfish, citing violations of statutes like the Computer Fraud and Abuse Act, the Federal Wiretap Act, the Stored Communications Act, the Electronic Communications Privacy Act, the California Invasion of Privacy Act, the North Carolina Unfair and Deceptive Trade Practices Act, trespass to chattels, common law fraud and negligent misrepresentation.

“The technology is moving so much faster than the legislatures can act," Meyer said. "And California is on the cutting edge, and even California is lagging behind."

--Editing by Jeremy Barker and Christine Chun.