LAW360

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

Data Breach Probes, Suits Will Test T-Mobile's Cyber Coverage

By **Shawn Rice**

Law360 (October 1, 2021, 11:06 AM EDT) -- T-Mobile's cyberinsurance coverage could be stretched by a recent data breach that has already spawned two government investigations and a slew of lawsuits by affected customers.

Since T-Mobile announced in August that more than 50 million of its customers had personal information stolen by cyber criminals**,** the U.S. wireless carrier has been hit with more than 30 suits as well as regulatory investigations by the Massachusetts attorney general's office and the Federal Communications Commission.

The ongoing fallout from the breach is expected to generate hefty legal bills for T-Mobile. The wireless carrier did not respond to a request for comment, but T-Mobile Chief Financial Officer Peter Osvaldik said at a conference hosted by Bank of America this month that his company has a "sizable cyberinsurance policy" that it expects will cover costs from potential regulatory probes and class action litigation.

Despite T-Mobile publicly acknowledging confidence in its cyber policy, Michael Miguel of McKool Smith, who represents policyholders, pointed out that companies' out-of-pocket costs for cyberattacks have skyrocketed. The cyber coverage likely isn't going to be at the levels T-Mobile is hoping for, based on the expected costs of responding to suits and regulatory investigations, he said.

Miguel noted that the Massachusetts attorney general has a reputation as one of the more aggressive state law enforcement officials. In the past, when the state's attorney general has succeeded in collecting substantial fines in probes against other companies, Miguel told Law360 that follow-on regulatory investigations have often resulted.

The attorney general's office, in a statement about its investigation, said it would be looking into how T-Mobile went about informing consumers of the data breach. The probe, led by the office's data privacy unit, will review T-Mobile's safeguards for protecting consumer information.

Representatives for the office declined to comment for this story.

Krishna Jani, a member of the cybersecurity and data privacy law practice at Flaster Greenberg PC, told Law360 that investigations "can often be very fact-sensitive and time-consuming." Still, in the midst of a pandemic with a large portion of the workforce operating remotely, Jani added, many businesses are doing the best they can with their cybersecurity measures and privacy protection.

"That may be a factor to consider in assessing violations and potential penalties," she said.

Miguel of McKool Smith said the question then becomes whether authorities can prove T-Mobile was behind the market in terms of its cyber protection controls. These types of regulatory investigations lead to more questions on what level of computer efficiency is required for corporate businesses to protect confidential data, he said.

"There is more to it than just the regulatory agency getting involved. Someone will have to set a standard on what governments and people expect that level of protection to be," he said. "From there, was that standard met or not? I wouldn't start counting my pennies that everyone will go out of business."

In the absence of comprehensive nationwide cybersecurity and data privacy legislation, experts said some states and federal authorities have stepped in to help provide a regulatory baseline for cybersecurity standards across the board. Regulators are inquiring more into the specific IT security measures companies have in place to mitigate cyber risks in response to the influx of cybersecurity incidents occurring during the pandemic, said Ericka Johnson, who's in the government investigations and white collar practice at Squire Patton Boggs.

For instance, in July, the New York Department of Financial Services issued cybersecurity guidelines in response to the rising threat of ransomware attacks. Some of these suggested measures included filtering emails to block spam, carrying out more training and exercises for employees, and stronger password systems.

The U.S. Securities and Exchange Commission, meanwhile, has said it wants publicly traded companies to disclose their cyber hygiene controls. In August, the SEC took action against a group of brokers and advisers, hitting them with hundreds of thousands of dollars in fines for taking inadequate steps to protect customer data.

At the same time, regulators in New York and at the Bermuda Monetary Authority have put more pressure on cyberinsurance carriers to implement stricter underwriting processes to help stop ransomware and other cyberattacks and to define the insured risk more accurately, according to experts.

Joshua Mooney of Kennedys, who represents insurance companies and corporations in data security compliance, told Law360 he anticipates more federal and state-level investigations like the ones against T-Mobile in the future.

Regulatory authorities are undertaking more oversight, with the threat of enforcement, over inadequate cybersecurity measures that could have mitigated or repelled a successful attack, as well as ransomware payments made in violation of requirements from the U.S. Treasury's Office of Foreign Assets Control and Financial Crimes Enforcement Network, Mooney added.

"The government and state regulators are telling carriers to incentivize policyholders to have more robust controls, which in effect is telling carriers to have higher premiums, tighter coverages and stricter processes, which courts never seem to like to hear," he said. "It also begs the separate question of whether it's fair to straddle the insurance industry with this responsibility."

Mooney compared this burden on cyber insurers to scenarios for insurers in other industries, like homeowners coverage, where insurers are told to compel homeowners to be more prepared for hurricanes and other climate events.

On top of the regulatory investigations, T-Mobile will incur substantial bills defending against the suits stemming from the breach. Many of these suits are proposed class actions filed on behalf of affected T-Mobile customers or credit applicants. T-Mobile recently asked a California federal court and Georgia federal court to pause two class actions until the Judicial Panel on Multidistrict Litigation decides whether to combine them with others.

There are concerns about public disclosures made by victimized companies to regulators being used in potential suits, Johnson of Squire Patton told Law360. But she said victimized companies should be proactive with regulators to set the narrative and show their diligence in responding.

Corporations like T-Mobile with a history of data breaches — the wireless carrier previously disclosed breaches in January 2014 and October 2015 — also will see an impact in the underwriting process for cyberinsurance coverage going forward, experts said.

A company that has been repeatedly hit like T-Mobile can expect to undergo a more rigorous underwriting process and must show they have adequate physical, administrative and technical data security controls, said Mooney of Kennedys. He told Law360 that there is an "emphasis and stress on accurately defining where the company stands on cybersecurity defenses."

Jani of Flaster Greenberg is currently seeing clients overhauling their internal security measures to ensure proper safeguards are in place. And other clients have asked for audits of their privacy policies, and other data protection measures, to ensure compliance with new and emerging laws, Jani said.

"Cybersecurity and data privacy are, or should be, on the forefront of every company's radar at the moment because cyberattacks are ramping up in terms of both frequency and sophistication," she said.

Increased cyberattacks and data breaches are happening just as the insurance market is in the peak of a hard cycle, said Michelle Chia, head of professional liability and cyber for Zurich North America. She told Law360 capacity is in low supply but in high demand, resulting in prices being driven up.

As businesses look to buy cyber coverage with the threat of more and more cyberattacks, Chia said organizations need to be resilient and learn what controls make their company "road ready." Companies are being asked to have response plans for data breaches and ransomware threats, Chia added.

"Having a decision tree and knowing how responsive and resilient you are is very important to that decision-making process," she said. "Like a fire drill, you practice so you're more prepared in the case of one."

--Additional reporting by Daphne Zhang, Nadia Dreid, Al Barbarino, Christopher Cole and Melissa Angell. Editing by Aaron Pelc.
