

# Privacy Daily

Under the terms of your subscription agreement, you may print one copy of an individual article for your own use. Please respect that limit.

---

## Lawyer Applauds Maine's Fast Response to False Data Breach Reports But Raises Validation Concerns

July 20, 2026 by Kara Thompson

The prompt action of the Maine attorney general's office after discovering it mistakenly posted two false data breach reports in June should protect the office's reputation, but the incident may spur regulators to be more aggressive in validation to avoid a repeat, a privacy lawyer told *Privacy Daily*.

This is the "first time we know of that" there has been a fake report sent to an AG office that was then published, Shook Hardy privacy lawyer Brandon Large said in an interview. Despite the office having to acknowledge it made a mistake, he doesn't think this incident "hurt[s] Maine's credibility."

The fact that the office "proactively took steps," reported that "they discovered an issue" and "disclosed it publicly ... actually demonstrates [that] they have active oversight of this situation," he said. "Obviously, the system wasn't perfect, but it may push them and maybe some other states to have these additional verification processes" for reported incidents.

This speaks to the idea that "transparency has real value, particularly in the eyes of attorneys general," and "they want their consumers to know that their data was breached," Large said. But "speed ... doesn't really always capture that objective," which is why validating "those breach response reports" from companies can be needed.

Though all AGs are different, "the goal really isn't choosing between transparency and accuracy, but really designing a system that can provide both to your consumers," the Shook Hardy lawyer said.

As of now, "this does not appear to be a widespread problem," he said. But Large is "surprised this hasn't happened before," as reporting a breach mainly consists of a company writing a letter to the regulator explaining what happened. There have been "other publicly facing reporting features that people have ... abused," like fake Securities and Exchange Commission filings or "hijacking social media platforms and making fake announcements."

"It's really hard to say" whether this will happen again, he said. "Whenever you have a reporting system that can become influential ... it could be a target for misuse." Large hopes that AG offices consider adding "an extra step of validation before they publish" these reports publicly.

### False Reports of Two Breaches

In mid-June, the Maine AG office announced “an apparent abuse” of the system resulting in false reports impacting video game platform VRChat and messaging platform Discord. The office said it has “no knowledge of any recent legitimate data breach reports from” the companies.

According to a LinkedIn post from internet security and cybercrime reporter Brian Krebs, the false reports claimed Discord had a breach impacting 10 million people, and VRChat had an incident affecting 2.5 million.

Though it removed the “hoaxes,” the public-facing database has been offline until the office can review its “procedures to make this abuse less likely in the future while preserving the public availability of such information,” the office said. Entities that need to submit breach reports are still able to do so through the same reporting service, it added.

Although many states require that breaches are reported to the AG or the appropriate state regulator, Maine is “unique,” Large told us. The state has a “low threshold” requiring the AG be informed if just one Maine resident is affected by a breach. Maine is also unique in that it is “one of the handful of states that ... publishes those reports” publicly.

---

Copyright© 2026 by Warren Communications News, Inc. Reproduction or retransmission in any form, without written permission, is a violation of Federal Statute (17 USC101 et seq.). Please review our [User Agreement](#).