

## Auto Insurer Settles With New York AG Over Insurance Application Platform Security Issues

Article By:

Liisa M. Thomas

Kathryn Smith

---

The New York Attorney General recently entered into an [assurance of discontinuance](#) with Root Insurance Company following a 2021 data incident. According to the AG, the threat actors obtained people's drivers' license numbers by exploiting a website error on its car insurance application portal. Namely, upon entering a publicly available name and address, the site would generate a prefilled PDF that included that person's drivers' license number, which numbers were pulled from third-party databases. Threat actors used an automated bot to exploit this vulnerability, and gathered drivers' license numbers of 44,449 New Yorkers (more than half of the total 72,852 people impacted). The threat actors then used many of these people's information to file fake unemployment claims with New York, which according to the AG, was the goal of the attack.

According to the AG, the company was not aware of the design feature issue. Instead, the situation was discovered when company personnel noticed unusual application activity. Upon discovery, the company took measures to address the issue, including using CAPTCHA to ensure the application was made by a human, and masking the license numbers. The AG nevertheless brought this case, claiming that the incident occurred because the company did not have appropriate risk assessment measures in place to identify the design error. It also should have, according to the AG, used measures like masking sensitive data and detecting and deterring automated traffic. These failures, it alleged, constituted a violation of the state's data security law, which requires that companies develop, implement and maintain "reasonable safeguards" to protect covered information. This information includes names and drivers' license numbers.

Similar to past settlements, the AG required that the company implement of additional security measures (see, for example, our posts about settlements with a [social media app last month](#), [ENT in December 2024](#), a [biotech company in mid-2024](#), and [Herff Jones in 2022](#)). Included in these are developing and maintaining a written information security program, designating a chief information security officer to oversee the program, engaging in network monitoring and employing multi-factor authentication, and maintaining compliance records for six years that the attorney general can access. The company has also agreed, among other things, to develop a data inventory, have a written process to ensure secure software development processes, to monitor network activity, and to promptly investigate suspicious activity. The company has also agreed to pay \$975,000.

**Putting it Into Practice:** This settlement outlines expectations from the New York attorney general of the proactive measures companies it believes companies should have in place if handling sensitive personal information. As companies launch new platforms, or revamp existing ones, this is a reminder to think not only about platforms where they collect personal information directly from individuals, but also where that information might be gathered from third party sources.

[Listen to this post](#)

Copyright © 2025, Sheppard Mullin Richter & Hampton LLP.

---

National Law Review, Volume XV, Number 94

Source URL: <https://natlawreview.com/article/auto-insurer-settles-new-york-ag-over-insurance-application-platform-security>