

RE: Data security event — Hippo Analytics Inc.

Good afternoon,

We are writing to inform your office about a data security incident. On August 3, 2026, Hippo Analytics Inc. (“Hippo”) determined it may have suffered a cybersecurity incident affecting nonpublic information. Hippo, through outside counsel, engaged an incident response firm and promptly began its investigation. After Hippo’s forensic investigation concluded, on October 9, 2026, Hippo determined that 5,132 MA residents were impacted, along with residents of other states.

Hippo maintains a public-facing website with an online quote tool that allows users to obtain insurance quotes by entering basic personal information. The quote tool utilized a “pre-fill” functionality that automatically retrieves additional consumer data from a third-party data service provider, Verisk, to verify information and improve the accuracy of automated quotes.

The investigation found that threat actors, operating through a commercial residential proxy network, were able to submit requests directly to Hippo’s pre-fill API and potentially receive enriched data back from the third-party service provider, possibly including driver’s license numbers. The investigation, however, despite multiple attempts and methodologies was unable to confirm whether any threat actors actually received this information.

This vulnerability traced back to a coding error in the design of Hippo’s prefill auto quoting tool that enabled the optional inclusion of driver’s license number fields. Hippo never intended to collect driver’s license numbers as part of prefill, and Hippo had no use for driver’s license numbers in its auto quoting workflow. The threat actors, however, discovered and exploited this legacy coding error.

Because the investigation was unable to correlate the unauthorized requests with any specific data returned, Hippo cannot definitively determine which specific individuals’ data was affected. Based on the forensic investigation, the unauthorized activity began on or about January 30, 2025 and continued until approximately August 11, 2026, when Hippo fully remediated the issue.

The types of personal information potentially at issue include name, driver’s license number, and date of birth. It is possible that the incident affected individuals with no prior relationship with Hippo, as the pre-fill tool could return information about any individual whose data was available from the third-party service provider.

Upon identifying the vulnerability and suspicious activity, Hippo promptly took the following steps:

- Removed the affected pre-fill API endpoints from the externally facing application, eliminating the ability for any user to query the pre-fill functionality through the quoting tool.
- Shut down the secondary backend service that also supported the vulnerable functionality.

- Removed the vulnerable mechanism in the quote tool that had been reported by a bug bounty researcher.
- Fully mitigated remaining potential risk through an additional code release on August 11, 2026, which removed all residual references to the affected pre-fill functionality from the application backend.

Hippo is also taking the following steps:

- Implementing CAPTCHA on all quote forms.
- Evaluating enhanced rate limiting, API authentication requirements, and enhanced logging and monitoring for anomalous query patterns.
- Enhancing security risk modeling and assessment for implementations.

Out of an abundance of caution, Hippo is notifying all MA residents whose information may have been returned during the period of unauthorized activity. Hippo is offering 12 months (or 24 months where required) of complimentary identity protection and credit monitoring services to affected individuals.

A copy of the individual notification letter is enclosed.

Should you have any questions please do not hesitate to contact outside counsel: Michael Bahar (MichaelBahar@eversheds-sutherland.com or +1.202.383.0882) or Alexander Sand (AlexanderSand@eversheds-sutherland.com or +1.512.721.2721).